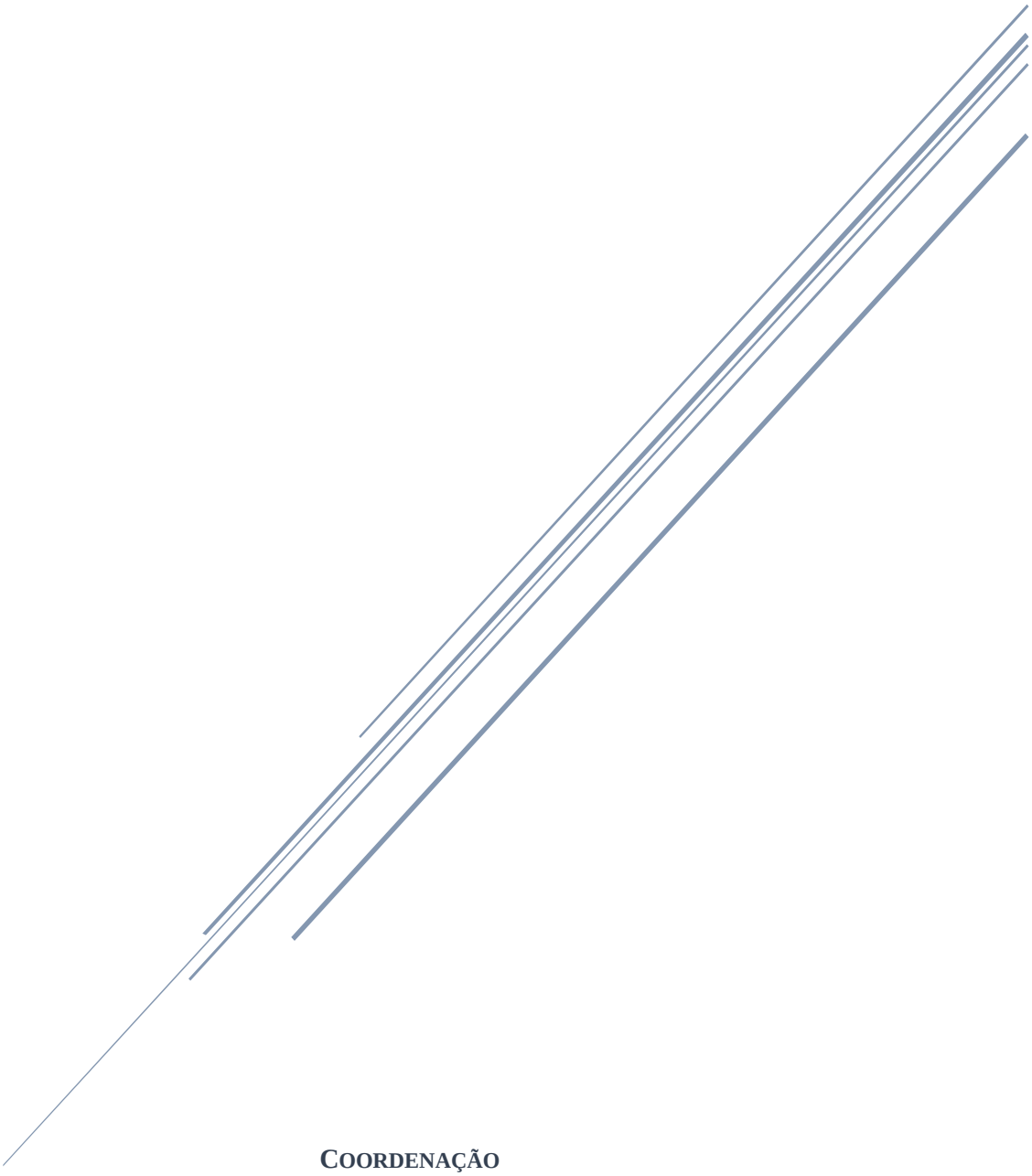
O RGPD E O IMPACTO NAS ORGANIZAÇÕES: 6 MESES DEPOIS. ATAS

X CONGRESSO INTERNACIONALDE CIÊNCIAS JURÍDICO-EMPRESARIAIS



COORDENAÇÃO
ANA LAMBELHO
JORGE BARROS MENDES

X CONGRESSO INTERNACIONAL
DE CIÊNCIAS JURÍDICO-EMPRESARIAIS

O RGPD e o impacto nas organizações: 6 meses depois

ATAS

COORDENAÇÃO:
ANA LAMBELHO
JORGE BARROS MENDES

FICHA TÉCNICA

Edição e Coordenação:
Ana Lambelho, IPLeiria
Jorge Barros Mendes, IPLeiria

Comissão Científica do X CICJE:
Ana Lambelho, IPLeiria
Jorge Barros Mendes, IPLeiria
Marisa Dinis, IPLeiria
Fernando Carbajo Cáscon, Universidade de Salamanca

Escola Superior de Tecnologia e Gestão
Instituto Politécnico de Leiria
www.cicje.ipleiria.pt

dezembro de 2019

ISSN: 2183-5330

NOTA DE PUBLICAÇÃO

O X Congresso Internacional de Ciências Jurídico-Empresariais (CICJE) decorreu na Escola Superior de Tecnologia e Gestão de Leiria, no dia 06 de dezembro de 2018, e foi subordinado ao tema "O RGPD e o impacto nas organizações: 6 meses depois".

As Atas que agora se publicam resultam das preleções dos oradores que compuseram os vários painéis. A todos os que contribuíram com os seus escritos para esta publicação e aos participantes no Congresso deixamos o nosso agradecimento.

Leiria, novembro de 2019

Os organizadores,

Ana Lambelho
Jorge Barros Mendes

Programa

09h30 Receção
09h45 Sessão de Abertura
Rui Pedrosa, Presidente do Politécnico de Leiria
Carlos Capela, Diretor da Escola Superior de Tecnologia e Gestão

Painel I Aspetos gerais do RGPD
10h00 RGPD nas organizações: a ecografia (possível) dos 6 meses
Angelina Teixeira, Advogada
10h20 O consentimento do titular de dados pessoais: requisitos e processo
Lurdes Dias Alves, UAL
10h40 GDPR impact on organisations - Six months on
Maria Flores, CIPP/E
11h00 *Coffee break*
11h20 O encarregado de proteção de dados
Margarida Ferreira, APDPO
11h40 A importância da segurança dos dados na internet
Mário Antunes, ESTG-IPLeiria
12h00 O papel da CNPD no RGPD
João Marques, CNPD
12h20 Debate
12h30 Almoço

Painel II – O RGPD no setor Público
14h00 Impacto nas Autarquias Locais, medido pelo acolhimento global
Rajani Oliveira, APAPP
14h20 O RGPD e o impacto nas organizações: 6 meses depois - o caso particular das instituições do ensino superior
Daniel Francisco, INA
14h40 A proteção de dados no sistema tributário português
Rui Zeferino Ferreira, ISVouga
15h00 A proteção de dados no direito português dos registos
Carlos Pedro, Conservador
15h20 Debate
15h30 *Coffee break*

Painel III – Aspetos práticos do RGPD
16h00 A implementação do RGPD numa organização - aspetos práticos
Jorge Barros Mendes, ESTG-IPLeiria
16h20 O RGPD no contexto laboral
Joana Janson e Joana Carneiro, Advogadas
16h40 As práticas de marketing online e o tratamento de dados pessoais do consumidor menor de idade
Rute Couto, IPB
17h00 Debate
17h15 Encerramento

Índice

Conteúdo

NOTA DE PUBLICAÇÃO 3
Programa 4
Painel I - Aspetos gerais do RGPD 6
RGPD nas organizações: a ecografia (possível) dos 6 meses 7
O Consentimento do Titular de Dados Pessoais: Requisitos e Processo 19
GDPR impact on organisations - Six months on 33
A importância da segurança dos dados na internet 39
Painel II – O RGPD no setor Público 47
Impacto nas Autarquias Locais, medido pelo acolhimento global 48
O RGPD e o impacto nas organizações: 6 meses depois - o caso particular das instituições do ensino superior 68
A proteção de dados no sistema tributário português 83
A proteção de dados no direito português dos registos 114
Painel III – Aspetos práticos do RGPD 117
O RGPD no contexto laboral 118
As práticas de marketing online e o tratamento de dados pessoais do consumidor menor de idade ... 135

Painel I - Aspetos gerais do RGPD

RGPD nas organizações: a ecografia (possível) dos 6 meses

Angelina Teixeira[1]

Sumário:

1. Introdução | **2.** Dos planos de aplicação do RGPD nas organizações | **3.** Breve alusão aos principais princípios ao tratamento de dados pessoais | **4.** Notas da ecografia – possível – dos 6 meses.

Resumo:

Este artigo visa contribuir para o conhecimento do impacto nas organizações decorridos 6 meses da entrada em vigor do novo Regulamento Geral de Proteção de Dados Pessoais e 2 anos depois da sua publicação. Se havia organizações que desconheciam o que era o RGDP, nos dias que antecederam o dia 25 de maio de 2018 ficaram a ter conhecimento pelo menos da sua existência. Apesar das dificuldades, dúvidas, imprecisões, interpretações diversas, desilusões, algum pânico, ressentiu-se em relação à proteção da privacidade e de segurança uma preocupação generalizada. Porém, apesar das tentativas de adaptação à nova forma de gestão dos seus dados, da formação e sensibilização para evitar violações inadvertidas das regras[2], registam-se ainda erros graves. A temática proposta será percorrida destacando as virtudes e potencialidades do Regulamento, incidindo num ou noutro tópico adjacente que venha a propósito, com particular destaque para as diferentes implicações ocorridas nas organizações, caracterizadas pelas duas faces da moeda.

Palavras-Chave: RGDP**,** proteção da privacidade, segurança, impacto nas organizações.

Abstract:

This article aims to contribute to the knowledge of the impact on organizations after 6 months of the entry into force of the new General Data Protecion Regulation and 2 years after its publication. If there were organizations that were not aware of what the GDPR was, I the days leading up to May 25, 2018 they become aware of at

[1] Advogada. angelinateixeira-53245P@adv.oa.pt

[2] A título exemplificativo vd. Hewlett-Packard Company. (2018). ***O que são as regras vinculativas das empresas (BCR -Binding Corporate Rules) da HP***. http://www8.hp.com/pt/pt/binding-corporate-rules.html

least its existence. Despite, difficulties, doubts, inaccuracies, various interpretations, disappointments, some panic, resented the protection of privacy and security a widespread concern. However, despite attempts to adapt to the new way of managing their data, training and awareness raising to avoid inadvertent violations of the rules, there are still serious errors. The proposed theme will be highlighted the virtues and potential of the Regulation, focusing on one or another adjacent topic that comes to the purpose, with particular emphasis on the different implications or organizations, characterized by the two sides of the coin.

Key-Words: *GDPR, privacy protection, security, impact on organizations.*

1. Introdução

"Dados são o novo petróleo, a inteligência artificial o motor" – Presidente Samsung na Web Summit

Agradecemos e louvamos a oportunidade que o Departamento de Ciências Jurídicas da Escola Superior de Tecnologia e Gestão, do Instituto Politécnico de Leiria e da Comissão Cientifica ESTG| IPLeiria nos proporcionou em termos de experiência e investigação ocorrida no X Congresso Internacional de Ciências Jurídico-Empresariais sob o tema "*O RGPD e o impacto nas organizações: 6 meses depois"*.

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 ou tão celebremente conhecido por Regulamento Geral sobre a Proteção de Dados (RGPD) veio, indubitavelmente alterar as organizações no que respeita ao tratamento dos dados pessoais dos titulares, seja na perspetiva dos seus clientes, trabalhadores, administradores ou gestores[3].

Tiveram assim, as organizações, até 25 de maio de 2018 para se adaptar às obrigações e procedimentos feitos pela União Europeia, exigência que contemplou todos os Estados-Membros, no que concerne à proteção das pessoas singulares, ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE[4].

---

[3] A ISO/IEC 27005:2011 "*A certificação do seu sistema de informação também pode levar a novas oportunidades de negócios com clientes preocupados com segurança, fortalecer a noção de sigilo em todo o local de trabalho e aumentar a ética dos funcionários. A certificação também permite que fortaleça a segurança da informação e reduza possíveis riscos de fraude, perda de informação e quebra de confidencialidade."* - https://www.iso.org/standard/54534.html

[4] A novidade da regulamentação surge por impulso das comunicações COM (2010) 609 final. *Uma abordagem global da proteção de dados pessoais na União Europeia*. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2010:0609:FIN e CE. (2012) e COM (2012) 11 final. *Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento*

Tem sido neste contexto que as organizações se têm vindo a deparar com vários desafios[5], exigindo destas uma série de adaptações de forma a evitarem aplicação de coimas [6] previstas no Regulamento, trazendo desta forma um "*novo paradigma".*

Hospital do Barreiro contesta judicialmente coima de 400 mil euros de Comissão de Dados

Comissão Nacional de Protecção de Dados aplicou multa por acesso irregular aos dados dos doentes. Situação tinha sido denunciada em Abril pelo Sindicato dos Médicos da Zona Sul.

TEMPESTADE LESLIE

Câmara de Lisboa usou base de dados da EMEL para enviar SMS de alerta

A introdução do RGPD no contexto europeu veio reforçar aquilo que há muito se previa, ou seja, a necessidade de um novo e real jurídico-legal sobre o seu direito fundamental à privacidade[7]. No plano nacional prevê a Constituição da República Portuguesa (CRP) nos seus artigos 26.º/1[8] e 35.º[9], parte integrante do capítulo dos

de dados pessoais e à livre circulação desses dados, in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0011:FIN. Aqui levantam-se uma série de questões, nomeadamente quanto à evolução tecnológica, globalização, melhoramento no processo de transparência de dados pessoais e proteção adequada dos titulares dos dados pessoais. Ver ainda, ANGELINA TEIXEIRA, A chave para a regulamentação da protecção de dados (das pessoas singulares), Data Venia, Ano 4, n.º 06 (Novembro 2016), http://www.dgsi.pt/bpjl.nsf/83cbe9acef94db5a8025730800549412/98d33869f73606f3802581d1005cdb52?OpenDocument

[5] Assembleia da República TV. (2016). *O Novo Regulamento Europeu de Proteção de Dados – Que desafios? Que oportunidades? – Sessão da Manhã: http://www.canal.parlamento.pt*

[6] O RGPD prevê a aplicação de coimas que podem ir até 4% do volume de negócios global anual ou 20 milhões de euros. Sendo que no ordenamento jurídico português, por força da aplicação do regulamento, a lei referente à proteção de dados, que ainda se encontra em debate, deverá implementar sanções especificamente aplicáveis às pequenas e médias empresas, e pessoas singulares. Na mesma linha, como o leitor saberá, continuamos a receber SMS e e-mails em massa em campanhas de marketing direto, sem que haja uma relação com a entidade remetente ou um prévio consentimento, não sendo, em muitos casos, respeitada a recusa em continuar a receber SMS ou e-mails ("opt-out").

[7] MANUEL DAVID MASSENO in https://www.academia.edu/37669646/Da_Privacidade_e_da_Prote%C3%A7%C3%A3o_de_Dados_enquanto_Limites_da_Prova_Digital_no_Direito_da_Uni%C3%A3o_Europeia

[8] Sob a epígrafe "Outros direitos pessoais" dispõe o artigo 26.º da CRP:

> 1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação*".*

[9] No contexto da legislação portuguesa, vem consagrado no artigo 35.º da CRP, o princípio da autodeterminação informativa, como desenvolvimento da personalidade, sendo um dos pilares fundamentais, o que se transcreve:

> *"*1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições

direitos fundamentais[10], o direito à reserva sobre a intimidade privada e o direito à utilização da informática[11]. Tais direitos refletem, nos dias de hoje, uma mudança de mentalidades que vai tendo reflexos, a título paradigmático, nas tão conhecidas e utilizadas redes sociais (considerando 6 e 7 do RGPD)[12].

Perante a necessidade de implementação do Regulamento aqui em análise, as organizações foram sentindo a necessidade de implementar[13], em matéria de dados pessoais, ferramentas de proteção num "todo" e para "qualquer" titular de dados pessoais[14].

aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei."

[10] Numa era de modernização, mudanças tecnológicas e afirmação do individuo enquanto cidadão de uma "aldeia global informatizada", é necessário assegurar em matéria de proteção de dados pessoais a aplicação da lei e prevenção da criminalidade – TIAGO MOREIRA, "O impacto do regulamento geral de proteção de dados nas organizações: um novo paradigma" – IPC, Maio 2018 in https://comum.rcaap.pt/bitstream/10400.26/23465/1/Tiago_Moreira.pdf , página 3.

[11] http://www.ministeriopublico.pt/pagina/vida-privada-utilizacao-da-informatica

[12] Como reflexo da conflitualidade de interesses entre os cidadãos e o Estado, sendo que no contexto europeu, devido à aplicação direta das normas europeias, todos os Estados-Membros, estão sujeitos à prevalência dos textos legais da União Europeia (UE) sobre as leis nacionais, tendo o RGPD o escopo de criar uma proteção mais sólida nesta matéria em prol dos cidadãos europeus. Neste contexto, veja-se os artigos 7.º e 16.º do Tratado sobre Funcionamento da União Europeia e o artigo 8.º da CDFUE, bem como a Convenção 108 de 1981 do Conselho da Europa para a Proteção das Pessoas Singulares relativamente ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, comummente conhecido pelo primeiro instrumento internacional na proteção de dados pessoais. Em Portugal, a autoridade administrativa independente e competente para controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados é a Comissão Nacional de Proteção de Dados (CNPD) in https://www.cnpd.pt/

[13] Recorda-se que os objetivos principais do RGPD passa por implementar nos Estados-Membros mecanismos legislativos aliados à contínua evolução tecnológica, aumentar a proteção dada a todos os titulares de dados pessoais às ameaças constantes e utilização indevida desses dados pelas organizações, e de complementar a iniciativa da UE relativamente ao Mercado Único Digital, no que promete ser uma novo mecanismo de oportunidades a todos os cidadãos europeus e Estados-Membros, desde que disponham das competências digitais necessárias - CE. (2018). Mercado Único Digital in https://ec.europa.eu/commission/priorities/digital-single-market_pt

[14] A proteção de dados pessoais, quer na sua dimensão física ou digital, requererá das organizações um reforço das medidas de proteção. Isto irá impor às organizações, quer multinacionais, quer pequenas e médias empresas um verdadeiro esforço, na monitorização dos fluxos de dados pessoais, controlo dos mesmos e o aumento do nível de alerta quanto aos riscos de privacidade - TIAGO MOREIRA, "O impacto do regulamento geral de proteção de dados nas organizações: um novo paradigma" – IPC, Maio 2018 in https://comum.rcaap.pt/bitstream/10400.26/23465/1/Tiago_Moreira.pdf , pág. 21.

2. Dos planos de aplicação do RGPD nas organizações

a) Âmbitos territorial e material

No âmbito da aplicação territorial dispõe o artigo 3.º/1 do RGPD que "ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União*."*

O RGPD, dada a sua dimensão de aplicação, abrange todas as organizações que estejam instaladas na UE, e fora desta, se o tratamento dos dados pessoais, como enuncia o art.º 3.º, n.º 1 do RGPD, sendo que o seu n.º 2 se aplica não só "ao contexto das atividades de um estabelecimento responsável pelo tratamento ou de um subcontratante," como também "ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante."

No ponto relativo ao tratamento de dados de titulares de residentes na UE, apenas se aplica o RGPD se as atividades de tratamento estiverem relacionadas com "a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares de dados procederem a um pagamento" e "o controlo do seu comportamento, desde que esse comportamento tenha lugar na União."

O mesmo será dizer que numa situação em que uma organização não esteja situada territorialmente na UE, mas que cuja atividade esteja direcionada para os consumidores residentes na UE, esta organização estará sujeita ao RGPD, nomeadamente as atividades direcionadas a sítios na internet[15]. Este alargamento do âmbito de aplicação territorial, conduz a que o tratamento seja mais equilibrado entre os responsáveis pelo tratamento de dados situados dentro e fora da UE.

Olhando para o âmbito de aplicação material, discorre o artigo 2.º/ 1 do RGPD que tem aplicação "ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados."

Neste sentido, o RGPD aplica-se a todas as formas de tratamento de dados pessoais, mesmo automatizadas. Significa assim que as organizações que realizem operações que envolvam dados pessoais, ficam abrangidas em razão de matéria,

[15] Tribunal de Justiça da União Europeia. (2015). ***Comunicado de Imprensa n.º 70/14.*** https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070pt.pdf

mesmo que o tratamento desses dados, seja "total ou parcialmente automatizados" e "não automatizados.[16]"

3. Breve alusão aos principais princípios ao tratamento de dados pessoais

Com a entrada do RGPD passamos a dispor de um leque reforçado de novos princípios, como sendo o princípio da licitude, da lealdade e transparência, espelho aliás da exigência do artigo 5.º, n.º 1, al. a) do Regulamento que impõe os dados pessoais devem ser "Objeto de um tratamento lícito, leal e transparente em relação aos titulares dos dados."

Em sintonia com os considerandos (4), (39), (58) e (59) do RGPD, os dados pessoais devem ser tratados de forma lícita, ou seja, "com base no consentimento do titular dos dados em causa"[17].

Impõe-se uma alusão, ainda que singela ao *princípio da lealdade* que determina que o tratamento dos dados pessoais deve ser de forma leal, ou seja, de acordo com o fim a que se destinam e não outro, fortalecendo a ligação entre a organização e o titular dos dados pessoais, ficando este último consciente de que os seus dados serão utilizados, compreendidos e salvaguardados pela entidade que os recolheu.

Por seu turno, o *princípio da transparência* reflete a conclusão de que o titular de dados pessoais, no que diz respeito, à recolha, utilização e consulta respeita "em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhe dizem respeito que estão a ser tratados."

Versando pelo artigo 5.º/1, b) do RGPD temos o princípio da *limitação das finalidades* determinado que os dados pessoais devem ser "Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento

[16] Por automatização de dados pessoais, entende-se como o processo em que a organização otimiza, a recolha e tratamento, com o objetivo de reduzir o esforço associado, e permitir executar as atividades relacionadas com os mesmos, em aplicações digitais, substituindo os processos manuais. Este processo de automatização resulta em maior eficácia na otimização, monitorização e controlo por parte da organização - Tiago Moreira, "O impacto do regulamento …", pág. 44.

[17] Efetuamos diversas pesquisas aos sítios da Internet de grandes empresas e outras não tão grandes que continuam a utilizar opções pré-preenchidas, quando o RGPD o proíbe taxativamente ao exigir um acto positivo de vontade, livre, expresso, esclarecido e inequívoco para valer como consentimento.

posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1."

Ora, face ao exposto, tal princípio impõe que a recolha dos dados, não deve ser utilizada para fim diferente daquele que inicialmente foi recolhido. Ou seja, o titular de dados pessoais, ao fornecer os seus dados, tem a plena consciência de que o tratamento irá ser de acordo com a finalidade inicial.

Percorrendo o artigo 5.º/1, agora na alínea c) é-nos dado a conhecer o *princípio da minimização dos dad*os que dá conta que os dados pessoais são: "Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados.". Na pática, aquando da recolha dos dados pela organização, decorre da obrigação da limitação – especifica - ao fim a que se destinam, não podendo ser usados para outro fim, ao qual o titular de dados pessoais não tenha consentido[18].

O *princípio da exatidão***,** conforme explana o artigo 5.º/1, d) do RGPD informar que os dados pessoais devem ser: "Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora."[19]

O princípio da *limitação da conservação*, segundo o art.º 5.º, n.º 1, al. e) do RGPD, que os dados pessoais são: "Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados

[18] O tratamento de dados pessoais para outros fins, deverá ser autorizado pelo titular dos mesmos dados, de forma assegurar a proteção necessária e a confidencialidade dos dados pessoais conservados. O conceito do consentimento, de acordo, com o art.º 4.º, n.º 11 do RGPD, define: "Uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento."

[19]As medidas adequadas a que se refere o artigo em questão, levam a que o responsável pelo tratamento de dados, quando exigido pelo titular desses dados pessoais, ter no imediato as ferramentas necessárias para a prossecução do cumprimento da exatidão e atualização dos dados inexatos. Como também a sua eliminação, ou retificação num prazo razoável, sem demora. Em jeito de sinopse, poder-se-á apontar de entre as medidas que as empresas devem continuar adotar, a criação de um sistema de registo de dados, revisão da política de privacidade, documentação, procedimentos e cumprimento do RGPD, organização dos direitos dos titulares dos dados, consciencialização das implicações do RGPD e ações de formação dos recursos humanos, adoção de medidas gerais que cumpram os requisitos de proteção, revisão e atualização das medidas de segurança do tratamento, revisão sobre as transferências transfronteiriças de dados. Sugere-se a leitura de MANUEL DAVID MASSENO, Da Proteção de Dados em Territórios Inteligentes: uma perspectiva desde as Fontes legislativas europeias e brasileiras - Comunicação, por videoconferência, ao I Congresso Internacional "Information Society and Law". Centro Universitário FMU, São Paulo. Dia 27 de novembro de 2018 in https://www.academia.edu/37859869/Da_Prote%C3%A7%C3%A3o_de_Dados_em_Territ%C3%B3rios_Inteligentes_uma_perspectiva_desde_as_Fontes_legislativas_europeias_e_brasileiras

durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados."

Os dados pessoais "devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados." Ou seja, até aqui, a prática comum das organizações, relativamente aos dados pessoais que recolhiam, seriam de certo modo, conservados por tempo indeterminado, ou até mesmo reproduzidos, para fins diferentes da suposta recolha inicial.

Podemos afirmar que com a entrada do novo RGPD há uma mudança de paradigma quanto a este princípio. Ou seja, os dados são recolhidos e limitados ao fim a que se destinam., devendo ser tratados até ao termo do período necessário para esse mesmo fim, exceto, a sua conservação poderá ser mais prolongada, se observar-se o disposto no art.º 5, n.1, al. e), *in fine* do RGPD.

Relativamente ao princípio da *integridade e confidencialidade* lê-se no artigo 5.º/ 1, al. f) do RGPD, que os dados pessoais devem ser: "Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas."[20] As medidas a adotar pela organização, de modo a implementar nas práticas de boa utilização dos dados pessoais dos titulares, devem obedecer ao princípio da integridade e confidencialidade – isto é, - a organização deve adotar medidas de proteção, que garantam a segurança dos dados pessoais contra possíveis invasões.

Seguramente nesta medida, tanto surgirá a proteção em termos físicos como digitais: físicos de modo a que não estejam ao alcance de quem não é legitimamente responsável pelo tratamento dos dados, como a proteção digital, segundo a aplicação de um sistema informático capaz de combater as "ações maliciosas ou ilícitas que

[20] Com a aplicação do RGPD, o responsável pelo tratamento de dados, no contexto organizacional, deve tomar medidas de modo a que as regras do referido regulamento, sejam aplicadas. Essas medidas organizativas, "devem ser revistas e atualizadas consoante as necessidades." As medidas, levam a que o responsável, possa garantir o nível de segurança desejado, dado que atinge todos os setores organizacionais, como por exemplo, no setor do marketing, tecnologias da informação, recursos humanos, administrativo, entre outros – página 58.

comprometam a disponibilidade, autenticidade, integridade e a confidencialidade dos dados pessoais conservados.[21]"

O *princípio da responsabilidade*, enuncia o art.º 5.º/2 do RGPD, que o responsável pelo tratamento de dados: "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo." O responsável pelo tratamento de dados, deve assegurar o cumprimento de todos os princípios enunciados anteriormente.

Esta responsabilidade aplica-se tanto ao responsável pelo tratamento como ao subcontratante, como se irá observar no Capítulo V. O responsável pelo tratamento, segundo o art.º 4.º, n.º 7 do RGPD entende-se como: "A pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro."

O subcontratante, define o art.º 4.º/8 do RGPD que "Uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes."

O RGPD vem, na prática, reforçar os deveres relativos ao subcontratante, nomeadamente quanto ao incumprimento das regras de proteção de dados pessoais[22]. A violação de dados pessoais, é definida como "uma violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público na Comunidade."[23]

A aprovação das regras vinculativas às empresas, devem seguir vários procedimentos de aprovação, de modo a escolher a Autoridade de Controlo Principal

[21] http://www.privacy-regulation.eu/pt/r49.htm

[22] Considerando (74), (79) e (81) do RGPD e https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_pt

[23]No Parecer 03/2014, relativo à notificação da violação de dados pessoais, emitido pelo GT29, "são fornecidas orientações aos responsáveis pelo tratamento, a fim de ajudá-los a decidir se devem ou não notificar as pessoas em causa, em caso de violação de dados pessoais."

(ACP)[24]. As regras aplicáveis às empresas[25], nas organizações multinacionais, que nomeadamente tenham um sítio na internet, por exemplo, divulgam as suas regras para dar conhecimento ao titular de dados pessoais, no que acontece em caso de transferência de dados[26].

Para facilitar o controlo do processo de transferência de dados pessoais numa organização multinacional, que transfira dados pessoais para um responsável ou subcontratante num país terceiro, é referenciado o *sistema de balcão único*, um mecanismo que possibilita a ACP, acompanhar todos os procedimentos que afetem tanto a organização principal como todos os outros estabelecimentos conexos, de modo a consolidar o nível de segurança adequado no tratamento de dados pessoais.

Os titulares de dados pessoais, além dos direitos apresentados quanto ao tratamento de dados pessoais, quando esses direitos são violados, podem os mesmos recorrer a ações judiciais que possam efetivar a defesa dos seus direitos e liberdades.

Este será porventura o maior receio das organizações, prevendo os artigos 83.º e 84.º do RGPD, a aplicação de coimas e consequentes sanções em caso de incumprimento das normas do regulamento.

4. Notas da ecografia – possível – dos 6 meses

Dúvidas parecem não restar que um dos temas que continua a merecer especial atenção é o da privacidade (ou a falta dela), seja ao nível da utilização tecnológica, online e das organizações e empresas de dados pessoais[27]. O Regulamento Geral sobre a Proteção de Dados é uma das maiores alterações de sempre relativamente à forma como deve ser realizado o tratamento de dados pessoais. O RGPD tem um impacto enorme em todos os departamentos de inúmeras

[24] CE. (2018). *Corporate rules for data transfers within multinational companies.*

[25] https://ec.europa.eu/justice/smedataprotect/index_pt.htm e https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_pt *"Do mesmo modo, as PME apenas terão de nomear um encarregado da proteção de dados se o tratamento for o seu principal negócio e constituir uma ameaça específica aos direitos e liberdades das pessoas (como o controlo de pessoas ou o tratamento de dados sensíveis ou registos criminais), sobretudo por ser efetuado em grande escala."*

[26] Tribunal de Justiça da União Europeia. (2015). ***Comunicado de Imprensa n.º 117/15*** declara inválida a decisão da Comissão que constatou que os Estados Unidos asseguram um nível de proteção adequado dos dados pessoais transferidos: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110pt.pdf

[27] Segundo a União europeia, o RGPD "estabelece regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE" in https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt

empresas e é muito provável que a maioria delas necessite de implementar práticas[28] e medidas de segurança para a sua própria salvaguarda contra ações de fiscalização.

Contudo, verifica-se que maior parte das empresas e outras entidades ainda não estão preparadas para a aplicação prática do RGPD e nem sabem como fazê-lo. No entanto, acreditamos que o RGPD se irá enraizar nas práticas diárias do setor empresarial a médio prazo. A decisão de mudar o paradigma na proteção de dados pessoais, é certamente, algo que veio tornar as organizações mais conscientes para esta temática. Neste sentido, a CE, de modo a analisar o impacto das novas tecnologias na vida dos cidadãos europeus, procedeu à recolha de dados sobre o conhecimento acerca desse impacto.

A análise ao RGPD permitiu constatar, uma alteração de paradigma. Um novo conceito. Um reforço do que já se conhecia, mas que agora, é definitivamente do conhecimento de qualquer cidadão da UE, de que o direito à proteção de dados pessoais se acaba de tornar uma consciencialização de que o tratamento, tanto pelas organizações como pelos titulares dos dados pessoais, está sujeito a responsabilidades e consequentes coimas. No conjunto de direitos do titular de dados pessoais, evidenciam-se, o direito ao consentimento e o direito a ser esquecido[29]. As organizações devem fornecer informações ao titular de dados pessoais acerca, das finalidades da recolha de dados pessoais. Sendo que essas informações devem abranger, se o tratamento assegura um nível adequado de proteção dos dados pessoais pelo responsável e subcontratante. Essas informações devem ser transparentes.

Recordamos que o Regulamento aqui em análise reconhece a própria evolução para um nível parco de segurança e onde a liberdade individual é colocada em causa (ex: Facebook, Instagram ou Twitter quando assumimos concordância com os "termos e condições")[30].

---

[28] A que se juntam reforço das regras e a constante necessidade de proteção dos titulares de dados pessoais que estejam ligados à organização, aliadas a novas medidas de sensibilização sobre a matéria de proteção de dados. O surgimento de uma nova profissão, o Encarregado de Proteção de Dados (EPD)[28] que passará a afigurar nos quadros da organização, para que as suas funções não surtam conflito de interesses.

[29] AUSLOOS, Jef. (2012). ***The right to be forgotten – Worth remembering?*** Computer Law & Security Review e MANUEL DAVID MASSENO, Do Direito ao Esquecimento na Sociedade da Informação: o Brasil entre os Estados Unidos e a União Europeia, https://www.academia.edu/36897211/Do_Direito_ao_Esquecimento_na_Sociedade_da_Informa%C3%A7%C3%A3o_o_Brasil_entre_os_Estados_Unidos_e_a_Uni%C3%A3o_Europeia https://www.sciencedirect.com/science/article/pii/S0267364912000246?via%3Dih%20ub

[30] Permitindo que essas plataformas digitais tenham acesso a informações pessoais que muitas vezes nem imaginamos que lhes estamos a dar, e isso não acontece só com essas empresas. Outro exemplo clássico encontramos nas nossas caixas de e-mail e na centena de vezes em que o nosso e-mail acaba em listas que não subscrevemos. Estas informações podem ser providenciadas gratuitamente *"por*

Cremos que a grande maioria das organizações (públicas ou privadas, grandes ou pequenas) em território nacional está ainda longe de estar preparado para as exigências decorrentes do novo regulamento que toca o ónus de responsabilidade do tratamento e da conformidade dos dados pessoais[31] – até então - da competência da Comissão Nacional de Proteção de Dados (CNPD).

Neste primeiro balanço, cabe ainda mencionar que muitas organizações continuam a ignorar as regras sobre a obtenção do consentimento dos titulares dos dados. As boas ou más reações dependem da postura (mindset) como se encara o RGPD. Se pensado que se destina a recolher mais impostos para os cofres do estado, sob a forma de coimas, então o resultado não poderá ser positivo. O RGPD não deve ser olhado como mais uma imposição ou custo acrescido, é certo que acarreta custos, mas isto fará com que, desde sempre, as regras do jogo que passa por derrotar a concorrência. Não será por obrado acaso que o RGPD se tem revelado como uma oportunidade inigualável para algumas organizações.

As contraordenações e respetivas coimas (60% - Estado, 40% - CNPD), possíveis crimes, penas de prisão, multas, as responsabilidades das pessoas singulares ou coletivas, as sanções acessórias, como a interdição temporária ou definitiva no tratamento, existem e nada mais são do que o exercício do poder legítimo do Estado: para quê?

Para ser cumprido!

escrito ou oralmente" a pedido do utilizador, com *"de forma concisa, transparente, inteligível e de fácil acesso"* e *"utilizando uma linguagem clara e simples"*. As pessoas devem ser informadas sobre se existem *"decisões automatizadas e a lógica envolvida, incluindo as suas consequências"*, no tratamento da informação.

[31] Pelo menos de forma completa e rigorosa.

O Consentimento do Titular de Dados Pessoais: Requisitos e Processo

Lurdes Dias Alves[1]

Sumário:

1. Notas introdutórias; 2. O consentimento; 3. Requisitos do consentimento; 3.1. Consentimento livre; 3.2. Consentimento específico; 3.3. Consentimento informado; 3.4. Consentimento explícito; 3.5. Declaração ou ato positivo inequívoco; 4. A irrelevância do consentimento do trabalhador no contexto laboral; 5. O caso especial do consentimento das crianças nos serviços da sociedade de informação; 6. Processo de consentimento; 6.1. Demonstração do consentimento; 6.2. Retirada do consentimento; 7. Considerações finais.

1. Notas introdutórias

Passados seis meses de plena aplicabilidade do Regulamento Geral de Proteção de Dados (RGPD), constata-se que a problemática em torno da obtenção do consentimento do titular de dados pessoais causou elevado impacto nas empresas e organizações, mas não só.

Este impacto também se tem feito sentir junto dos titulares de dados pessoais, que nem sempre se sentem devidamente esclarecidos sobre quando, como e porque devem dar consentimento para o tratamento dos seus dados, e como e quando podem retirar o consentimento anteriormente dado.

Para que qualquer tratamento de dados seja lícito – logo válido, tem de ter por base um fundamento jurídico. À semelhança do que já se verificava na Diretiva 95/46/CE[2] (que o RGPD[3] mantém inalterável), o regulamento para efeitos de licitude

[1] Licenciada em Direito pela Universidade Autónoma de Lisboa. Pós-graduada em Direito Comercial e Direito Societário pela Universidade Católica Portuguesa – Escola de Lisboa. Mestre em Direito (especialidade de Ciências Jurídicas) pela Universidade Autónoma de Lisboa. Doutoranda em Direito (especialidade de Ciências Jurídicas) na Universidade Autónoma de Lisboa, onde investiga o tema: "*A proteção de dados pessoais e o sigilo bancário – A derrogação da privacidade*". Investigadora integrada no RATIO LEGIS - Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa. Cocoordenadora de Pós-Graduações em Proteção de Dados Pessoais, Privacidade e Cibersegurança na UE, na Autónoma Academy (Escola de Pós-graduações da Universidade Autónoma de Lisboa).

[2] DIRETIVA Nº 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO, de 24 de outubro de 1995. *Jornal Oficial das Comunidades Europeias*. (23.11.95). Doravante abreviadamente designada por DIRETIVA Nº 95/46/CE ou Diretiva.

[3] REGULAMENTO (UE) Nº 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016. ***Jornal Oficial da União Europeia***. PT (4.5.2016). Doravante abreviadamente designado por REGULAMENTO ou RGPD.

do tratamento de dados pessoais requer que se verifiquem, pelo menos, uma das seguintes situações: além do consentimento, a necessidade do tratamento para efeitos de execução contratual, cumprimento de uma obrigação jurídica, defesa de interesses vitais do titular dos dados ou de terceiro, exercício de funções de interesse público, ou ainda em caso de um interesse legítimo prosseguido pelo responsável pelo tratamento, desde que, neste caso, não prevaleçam interesses, direitos ou liberdades fundamentais do titular[4].

Assim, o consentimento[5] continua a ser um dos seis fundamentos legais para aferir a legitimidade do tratamento de dados pessoais. Em regra, só se poderá considerar que o consentimento constitui fundamento legal apropriado se ao titular dos dados pessoais for dada a oportunidade de controlo dos seus dados e desde que se verifique sempre a opção de aceitar ou recusar que os seus dados sejam tratados nos termos que lhe são apresentados - com a opção clara de que poderá recusar o tratamento dos seus dados, sem que venha a ser prejudicado pela sua opção de recusa.

A Diretiva 95/46/CE definiu o consentimento como: "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento.[6]", e que tiver sido "dado de forma inequívoca"[7]. Não obstante, o RGPD alargou o leque de requisitos para a verificação do consentimento, acrescentando[8] que a manifestação de vontade tem de ser "*explícita*"[9]. Além deste «novo» requisito, denote-se que o consentimento sai reforçado no regulamento, por se exigir que aquele seja demonstrado "*mediante declaração"* ou "*ato positivo inequívoco"*.

[4] Nos termos do art.º 6.º do RGPD.
[5] Alguns autores consideram até que o consentimento constitui a «espinha dorsal» do tratamento de dados pessoais; neste sentido, veja-se por exemplo REBOLLO, Lucrecio – *Protección de datos en Europa: origen, evolución y regulación actual*. Madrid: Editorial Dykinson, 2018. p. 112 e ss..
[6] Conforme alínea h) do art.º 2.º da DIRETIVA Nº 95/46/CE. *Idem*.
[7] De acordo com a alínea a) do art.º 7.º da DIRETIVA Nº 95/46/CE. *Ibidem*.
[8] Conforme n.º 11 do art.º 4.º do RGPD.
[9] Uma especial chamada de atenção para a definição de consentimento na versão inglesa do RGPD: '*consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*. Onde a manifestação de vontade que concretiza o consentimento tem de ser "*unambiguous indication of the data subject's*" e não explícita, utilizando somente tal requisito quando se esteja perante o tratamento de dados sensíveis – dados de saúde, dados biométricos ou de decisões individuais automatizadas. A versão Portuguesa do RGPD «exige taxativamente» que seja uma manifestação de vontade explícita, independentemente dos dados pessoais a tratar serem dados sensíveis ou não.

2. O consentimento

O RGPD[10], apesar de encerrar em si muitos princípios, regras gerais, direitos e obrigações que já constavam da Diretiva 95/46/CE[11], veio realmente introduzir importantes alterações: entre outras, e talvez a mais notória em termos jurídicos, intensificou o processo e requisitos aplicáveis à obtenção do consentimento do titular de dados pessoais nas mais diversas operações de tratamento de dados, fomentando a obrigatoriedade de demonstrar se o consentimento obtido pelo responsável pelo tratamento respeita todos os novos requisitos – em caso negativo, será imprescindível obter novo consentimento do titular dos dados pessoais em conformidade com as disposições do RGPD, sob pena de o tratamento se tornar ilícito por falta de fundamento jurídico[12].

3. Requisitos do consentimento

Estabelece o n.º 1 do art.º 6.º do RGPD, quanto aos requisitos conducentes à verificação da licitude para o tratamento de dados pessoais, que o tratamento é lícito se o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas.

E se o tratamento for necessário para: **(i)** a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; **(ii)** o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; **(iii)** a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; **(iv)** o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; **(v)** efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros[13], exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

---

[10] REGULAMENTO. *Ob. Cit.*
[11] DIRETIVA Nº 95/46/CE. *Ob. Cit*.
[12] Ressalva-se a proibição do tratamento das categorias especiais de dados pessoais, a que alude o preceituado no n.º 1 do art.º 9.º (RGPD) "*É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa*".
[13] Porém, exclui-se o tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

O próprio ato de uma organização solicitar ao titular dos dados pessoais a aceitação de uma operação de tratamento de dados, dando o seu consentimento, está sujeito a requisitos rigorosos[14], sujeição justificável porque estão em causa direitos fundamentais dos titulares dos dados e o responsável pelo tratamento tem que evitar efetuar uma operação de tratamento que não seria lícita sem o consentimento do titular. É dado especial relevo ao papel crucial do consentimento nos art.ºs 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, que consagra o respeito pela vida privada e familiar e a proteção de dados pessoais[15].

O RGPD salvaguarda exigências adicionais para o consentimento válido - como é o caso da capacidade legal: naturalmente, no contexto da proteção de dados terá sempre de se ter em conta os preceitos da lei civil para suprimento das incapacidades, uma vez que os requisitos do Regulamento consubstanciam pré-requisitos legais fundamentais. O consentimento inválido de pessoas que não tenham capacidade legal resultará portanto na ausência de uma base legal para o tratamento de dados sobre essas pessoas[16].

Não obstante, a obtenção do consentimento não reduz nem decresce as obrigações do responsável pelo tratamento de dados pessoais, no que concerne à observância dos princípios relativos àquele tratamento consagrados no RGPD[17].

Ainda que o tratamento dos dados pessoais se alicerce no consentimento do titular dos dados, este facto, não legitima a recolha de dados que não seja necessária para a finalidade específica do tratamento - e muito menos para tratamentos que sejam fundamentalmente desleais.

---

[14] Conforme orientações do GRUPO DE TRABALHO DO ARTIGO 29.º. *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*. [Em linha]. Adotadas em 28 de novembro de 2017. (Última redação revista e adotada em 10 de abril de 2018. [Consultado em 20 mai. 2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf.

[15] CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA, de 7 de dezembro de 2000. *Jornal Oficial da União Europeia*. PT (30.3.2010), "Art.º 7.º - Respeito pela vida privada e familiar - Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações; Art.º 8.º - Protecção de dados pessoais - 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente." (sublinhado nosso).

[16] De acordo com EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE 2018 – *Handbook on European data protection law*. 2018 edition. Luxembourg: Publications Office of the European Union, 2018.

[17] Princípios estabelecidos no art.º 5.º do RGPD, nomeadamente os princípios da: licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade.

Atente-se, pois, que a legitimidade para o tratamento de dados pessoais advém da licitude na obtenção do consentimento do titular dos dados, e este consentimento somente é lícito - logo válido - se corresponder a uma "*manifestação de vontade*, *livre*, *específica*, *informada* e *explícita"*, pela qual o titular dos dados aceita o tratamento "*mediante declaração"* ou "*ato positivo inequívoco"*. Importante será salientar o facto de que não é aceitável que o pedido de consentimento seja apresentado de forma genérica – tem de ser apresentado num contexto restrito[18] fixando as finalidades – claramente definidas e concretas e separadas de outras informações[19].

3.1. Consentimento livre

O requisito de um consentimento livre impõe que se verifique uma verdadeira escolha e controlo dos seus dados, por parte do respetivo titular. O RGPD prevê que caso não seja dada ao titular dos dados a oportunidade de exercer uma verdadeira escolha, de consentir ou não, caso seja coagido a dar o consentimento, ou ainda caso existam implicações negativas se não consentir, o consentimento prestado não é válido[20].

Para proceder à avaliação sobre se o consentimento foi dado livremente, a primeira análise a ter em conta é saber se o consentimento está subordinado à execução de um contrato ou à prestação de um serviço[21], se estamos perante uma situação de desequilíbrio de poder[22]; depois, se os dados envolvem múltiplas

[18] A título meramente exemplificativo, vejamos o consentimento dado por um paciente a uma determinada unidade de cuidados de saúde: o paciente, titular dos dados pessoais, dá o seu consentimento para que os seus dados sejam do conhecimento de vários profissionais de saúde integrados numa equipa multidisciplinar de assistência em saúde - e esta é a finalidade única para o tratamento dos seus dados de saúde, sobre o contexto restrito da finalidade do tratamento e a proteção de dados de saúde, DEODATO, Sérgio – *A Proteção dos Dados Pessoais de Saúde*. Lisboa: Universidade Católica, outubro de 2017, que seguimos.

[19] Porque no caso em que o tratamento de dados pessoas sirva diversas finalidades, terá de ser dado consentimento, separadamente, para cada uma dessas finalidades.

[20] Caso o consentimento esteja associado a uma parte não negociável das condições gerais de um contrato, é de presumir que foi dado livremente pela parte inegociável das condições gerais. O Regulamento prevê que não se pode considerar que o consentimento foi dado de livre vontade se ao titular dos dados não for dada a opção de recusar nem a faculdade de o poder retirar sem que de tal vontade advenha uma consequência negativa. Por este motivo se compreende que o RGPD tenha tido em consideração esta noção de desequilíbrio entre o responsável pelo tratamento e o titular dos dados.

[21] Como descrito no n.º 4 do art.º 7.º do RGPD.

[22] O considerando 43 do RGPD determina: "A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. […]", logo, revela claramente a impossibilidade de utilizar o consentimento para o tratamento quando o responsável pelo tratamento for uma autoridade pública, dado que na generalidade dos casos se estará perante um manifesto desequilíbrio de poder na relação entre o responsável pelo tratamento e o titular dos dados.

operações de tratamento[23], e se são para mais que uma finalidade[24], e por último demonstrar que ao titular dos dados pessoais foi oferecida a possibilidade de recusar ou retirar o consentimento sem que lhe advenham, dessa sua livre manifestação de vontade, prejuízos ou consequências nefastas[25].

3.2. Consentimento específico

Da alínea a) do n.º 1 do artº 9.º do RGPD retira-se a confirmação de que o consentimento do titular dos dados pessoais deve ser dado em relação a *"(…) uma ou mais finalidades específicas*" e que o titular tem a livre escolha em relação a cada uma delas. O requisito de que o consentimento deve ser específico destina-se a asseverar um determinado grau de controlo e transparência em relação ao titular dos dados pessoais. Assim, para que se verifique o cumprimento do requisito de que o consentimento deve ser específico, o responsável pelo tratamento de dados pessoais deve assegurar uma verdadeira especificação em função da finalidade e garantir que os pedidos de consentimento para finalidades diversas são efetuados separadamente, e não para um conjunto de finalidades de tratamento; note-se ainda que deve existir uma separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões.

---

[23] Sabendo que uma determinada recolha de dados pessoais pode envolver múltiplas operações de tratamento e para diversas finalidades, aos titulares dos dados tem de ser dada a opção de escolha para que finalidades dão consentimento, e não pode o responsável pelo tratamento de dados solicitar um consentimento conjunto para diversas finalidades; terão de ser solicitados tantos consentimentos quantos forem as finalidades de tratamento. Neste sentido, o considerando 32 clarifica que: *"(…) O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins (…)".*

[24] O responsável pelo tratamento de dados, ao impor a obrigatoriedade de concordância com a utilização de dados pessoais além da utilização estritamente necessária, condiciona a livre escolha do titular dos dados e obstaculiza a livre vontade do ato de consentir.

[25] Cf. considerando 42 do RGPD: "Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. (…) uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.", Sobre o responsável pelo tratamento impende a obrigatoriedade de demonstrar que a retirada do consentimento não implica quaisquer custos para o titular dos dados e, nem qualquer desvantagem.

3.3. Consentimento informado

O RGPD reforça o requisito de que o consentimento deve ser informado. Desde logo, o requisito de transparência é um dos princípios fundamentais, diretamente relacionado com os princípios da lealdade e da licitude[26]. Este requisito torna necessário o fornecimento de todas as informações aos titulares dos dados pessoais antes da obtenção do consentimento, para que estes possam tomar decisões informadas. De referir que estas informações têm de ser apresentadas *"de uma forma que o distinga claramente de outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples*[27]**"**, e incluir a informação de que os titulares dos dados podem exercer o direito de retirar o consentimento dado.

Caso o responsável pelo tratamento não forneça informações acessíveis, o consentimento será um fundamento inválido para o tratamento[28]. Verifica-se que o consentimento é informado quando o responsável pelo tratamento dos dados pessoais informe ou coloque à disposição do titular dos dados, pelo menos, a seguinte informação, porque esta é necessária para a obtenção de um consentimento válido: **(i)** identidade do responsável pelo tratamento; **(ii)** a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento; **(iii)** que (tipo de) dados serão recolhidos e utilizados; **(iv)** existência do direito de retirar o consentimento; **(v)** informações acerca da utilização dos dados para decisões automatizadas em conformidade com a alínea c) do n.º 2 do art.º 22.º do RGPD[29]; e **(vi)** sobre os possíveis riscos de transferências de dados devido à inexistência de uma decisão de adequação e de garantias adequadas, tal como previsto no art.º 46.º do RGPD.

O Regulamento não define nem a forma nem o formato em que as informações devem ser prestadas e disponibilizadas ao titular dos dados para o cumprimento do requisito de consentimento informado; logo, deixa em aberto um leque de

[26] Cf. art.º 5.º do RGPD.
[27] Nos termos do n.º 2.º *in fine* do art.º 7.º do RGPD.
[28] A consequência do não cumprimento do requisito de consentimento informado é a invalidade do consentimento, e neste caso, o responsável pelo tratamento estará a violar o disposto no art.º 6.º do RGPD.
[29] Assegura o RGPD que os titulares de dados pessoais têm o direito de não ficar sujeitos a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, exceto se for baseada no consentimento explícito do titular dos dados; logo para que livremente o titular dos dados pessoais possa dar o seu consentimento explícito – tem de estar informado.

possibilidades para a apresentação de informações válidas, que podem ser declarações escritas ou orais, mensagens áudio ou vídeo[30].

3.4. Consentimento explícito

Um outro requisito necessário para a verificação da validade do consentimento, é o requisito de que o consentimento tem de ser explícito, desde logo porque o consentimento explícito é necessário em determinadas situações em que surge - ou é previsível poder ocorrer - um risco grave para a proteção dos dados e, por conseguinte, quando se considera adequado existir um nível elevado de controlo por parte do titular dos dados pessoais.

Nos termos do RGPD, o consentimento explícito assume um papel determinante para o cumprimento dos requisitos a que alude o art.º 9.º, relativo ao tratamento de categorias especiais de dados pessoais, seja nas disposições sobre transferências de dados para países terceiros ou organizações internacionais, na ausência de garantias adequadas preceituadas no art.º 49.º, assim como no art.º 22.º relativamente a decisões individuais automatizadas, incluindo a definição de perfis.

3.5. Declaração ou ato positivo inequívoco

O Regulamento prevê uma declaração ou ato afirmativo inequívoco como requisito prévio do consentimento "*conforme às regras*"[31]. Dado que, no RGPD, o requisito de consentimento "*conforme às regras*" é mais exigente do que o requisito de consentimento que consta da Diretiva 95/46/CE, importa clarificar quais são os esforços adicionais que o responsável pelo tratamento de dados pessoais deve diligenciar para a obtenção de um consentimento explícito do titular dos dados pessoais e em conformidade com o Regulamento.

Por fim, outro dos requisitos do consentimento exigidos no RGPD é a manifestação de vontade inequívoca, e o Regulamento expressa de forma clara a

[30] Todavia, o Regulamento estabelece vários requisitos para o consentimento informado (veja-se o n.º 2 do art.º 7.º e considerando 32 do RGPD), esta questão implica maior exigência quanto à clareza e acessibilidade das informações.

[31] Para que o responsável pelo tratamento obtenha uma declaração ou ato positivo inequívoco» para a verificação dos requisitos do consentimento explícito, esta em primeiro lugar deve manifestar expressamente o consentimento, que pode ser obtido mediante uma declaração escrita e assinada pelo titular dos dados, de forma a eliminar todas as dúvidas possíveis (*v.g.* uma potencial falta de provas no futuro), porém a forma de declaração escrita não é a única forma para a obtenção do consentimento explícito (nem tão pouco o RGPD recomenda declarações escritas e assinadas em todas as circunstâncias que exigem um consentimento explícito válido). Em contexto digital o titular de dados pode emitir a declaração necessária preenchendo um formulário eletrónico; enviando uma mensagem de correio eletrónico; carregando um documento digitalizado com a assinatura do titular dos dados ou utilizando uma assinatura eletrónica, a título exemplificativo.

exigência de uma ação por parte do titular dos dados pessoais, concretizada numa declaração ou um ato positivo inequívoco; tal ação tem de ser manifestada de modo inteligível e implicar sem qualquer margem para dúvida que o titular quis, efetivamente, dar o seu consentimento[32].

4. A irrelevância do consentimento do trabalhador no contexto laboral

No contexto laboral, por norma, o consentimento do trabalhador não é considerado um fundamento válido para o tratamento de dados pessoais, face à finalidade em causa e considerando a posição de dependência e subordinação do trabalhador; entende-se, pois, que este poderá não estar em posição de conceder o seu consentimento nos termos exigidos pelo RGPD, onde se prevê que tal consentimento seja prestado livremente e que seja tão fácil de retirar como de conceder, sem que daí advenham quaisquer consequências para o trabalhador.

A relação empregador-trabalhador é, de um modo geral, considerada uma relação de desequilíbrio[33], na qual o empregador possui supremacia em relação ao trabalhador. Uma vez que o consentimento tem de ser dado de livre vontade, e tendo em conta a natureza da relação laboral, o empregado, não pode, na maioria dos casos, basear-se no consentimento para utilizar os seus dados. Contudo, poderão existir situações em que o tratamento dos dados pessoais de um trabalhador, com base no respetivo consentimento, seja lícito, especialmente se esse tratamento for do interesse do próprio trabalhador.

O direito interno, as convenções coletivas ou os acordos setoriais podem estabelecer regras específicas sobre o tratamento de dados pessoais no contexto laboral; porém, o trabalhador pode dar o seu consentimento para o tratamento dos

[32] Neste ponto, a alínea h) do art.º 2.º, da Diretiva 95/46/CE define consentimento como "manifestação de vontade (...), pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento". Porém, o RGPD vai mais longe e no n-º 11 do art.º 4.º amplia esta definição, exigindo que, para que se verifique um consentimento, seja necessário que o responsável pelo tratamento dos dados pessoais obtenha do titular uma manifestação explícita mediante declaração ou ato positivo inequívoco, manifestação esta que pode ser concretizada através da obtenção de uma declaração escrita ou oral (gravada), inclusivamente em formato eletrónico.

[33] Considera-se uma relação de desequilíbrio inerente à dependência que resulta da relação empregador/trabalhador, perante a improbabilidade da recusa do titular dos dados dar o seu consentimento para o tratamento, sem que haja medo ou risco real de consequências negativas decorrentes da recusa, a livre manifestação de vontade podendo obstar à continuidade da relação laboral. Essa improbabilidade de recusa verificar-se-á por exemplo perante o pedido de consentimento para a ativação de sistemas de controlo como a vigilância do local de trabalho através de câmaras, ou, num outro exemplo, no preenchimento de formulários de autoavaliação. Assim, o fundamento legal para o tratamento de dados no local de trabalho, não pode nem deve ser o consentimento dos trabalhadores (alínea a) do n.º 1 do art.º 6.º do RGPD).

seus dados, nomeadamente, para efeitos de "recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas por lei ou por convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no trabalho, de saúde e segurança no trabalho, e para efeitos de exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.[34]"

O Regulamento contempla esta possibilidade da criação de regras ou normas específicas para o tratamento de dados pessoais, quer pelo direito interno, quer pelas convenções coletivas (incluindo os acordos setoriais), para que seja garantida a defesa dos direitos e liberdades no tratamento de dados pessoais dos trabalhadores. Contudo, estas regras ou normas específicas devem ter medidas que visem salvaguardar[35]: **(i)** a dignidade; **(ii)** os interesses legítimos; **(iii)** os direitos fundamentais do titular dos dados; **(iv)** a transparência do tratamento de dados; **(v)** a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta; e, **(vi)** os sistemas de controlo no local de trabalho[36].

5. O caso especial do consentimento das crianças nos serviços da sociedade de informação

O consentimento enquanto fundamento jurídico para o tratamento de dados pessoais de crianças com idade inferior a 16 anos, para que seja lícito, carece ainda da obtenção do devido consentimento junto dos titulares das responsabilidades parentais. O RGPD[37] prevê, no que concerne à oferta direta de serviços da sociedade da informação, em particular no contexto de serviços de internet (*v.g*. redes sociais), uma proteção especial para o tratamento de dados pessoais relativos a crianças com idade inferior a 16 anos. Todavia, a Lei Nacional de Execução poderá, ainda, estabelecer uma idade inferior que permita às crianças com idades inferiores a 16 anos darem o seu consentimento; de notar, contudo, que o regulamento salvaguarda o limite mínimo de 13 anos.

---

[34] Cfr. considerando 155) e n.º 1 do art.º 88.º do RGPD.
[35] Nos termos do n.º 2 do art.º 88º do RGPD.
[36] Os trabalhadores estão hoje sujeitos a um grande número de controlos específicos, e a uma supervisão praticamente contínua de cada trabalhador com forte incidência na sua privacidade. Entre os sistemas de controlo no local de trabalho, destacamos: sistemas biométricos para controlo de assiduidade; controlos de alcoolemia ou de substâncias psicoativas; controlos médicos; sistemas de controlo da utilização dos telefones, do correio eletrónico, do acesso à Internet ou do computador; sistemas de geolocalização; e sistemas de videovigilância.
[37] Em conformidade com o art.º 8.º do RGPD.

Naturalmente, o RGPD confere proteção adicional a este tipo de dados, porque as crianças, pela falta de maturidade inerente à sua inexperiência, são inscientes quanto aos riscos e às consequências da partilha dos seus dados pessoais, do mesmo modo que não têm o cientificismo necessário para aferir os seus direitos. Qualquer informação dirigida especificamente a uma criança deve ser facilmente acessível e formulada numa linguagem clara e simples, muito embora para os serviços tecnológicos disponíveis seja necessário o consentimento e autorização do titular das responsabilidade parentais para a realização do tratamento de dados pessoais de uma criança com base no consentimento até uma determinada idade[38].

O Regulamento veio ainda introduzir obrigações suplementares que visam asseverar um reforço quanto à proteção dos dados das crianças relativamente aos serviços da sociedade da informação, justificável porque as crianças "(…)podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. (…)[39]" estabelecendo ainda que "Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças."

6. Processo de consentimento

Um pedido de consentimento tem de ser apresentado ao titular dos dados pessoais de forma clara e concisa, utilizando uma linguagem de fácil compreensão, e de modo que o distinga claramente de outras informações, como os termos e condições do serviço. O pedido tem de especificar qual a utilização que será dada aos dados pessoais recolhidos e tem de incluir os contactos do responsável pelo tratamento de dados.

O consentimento tem de ser dado de livre vontade e tem de ser específico e informado, através de uma manifestação de vontade positiva, de forma inequívoca.

[38] Este procedimento tem de ser válido tanto para as redes sociais, como para plataformas de transferência de música e compra de jogos em linha. Salienta-se que os serviços preventivos ou de aconselhamento (*v.g.* SOS criança e muitas outras) oferecidos diretamente a crianças estão isentos do requisito de consentimento parental, uma vez que visam proteger o interesse superior da criança.
[39] Cfr. considerando 38) do RGPD.

6.1. Demonstração do consentimento

Para que se considere que o consentimento é informado, o responsável pelo tratamento tem de demonstrar que o titular dos dados recebeu, pelo menos, as seguintes informações sobre o tratamento: **(i)** a identidade do responsável pelo tratamento dos dados; **(ii)** os fins para os quais os dados irão ser tratados; **(iii)** o tipo de dados que serão tratados; **(iv)** a possibilidade de retirar o consentimento dado (*v.g*., enviando uma mensagem de correio eletrónico para retirar o consentimento); **(v)** se aplicável, o facto de os dados irem ser utilizados para decisões exclusivamente automatizadas, incluindo a definição de perfis; **(vi)** informações destinadas a apurar se o consentimento está relacionado com uma transferência internacional dos dados, bem como os possíveis riscos de transferências de dados para fora da UE, se tais países não estiverem sujeitos a uma decisão de adequação da Comissão e não existirem garantias adequadas.

Preceitua o n.º 1 do art.º 7.º do RGPD que impende sobre o responsável pelo tratamento de dados pessoas a obrigatoriedade de demostrar que o titular dos dados deu o seu consentimento, sendo que "*sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados*.[40]"

Deste modo, verifica-se que o Regulamento deixa aos responsáveis pelo tratamento de dados pessoais a liberdade para desenvolver procedimentos que visem o cumprimento da demonstração da obtenção do consentimento; porém, para o cabal cumprimento desta obrigação do responsável pelo tratamento, não devem ser solicitados excessivos dados para tratamento adicional, *i.e.*, apenas devem ser recolhidos os dados suficientes para mostrar a validade para o tratamento (mostrar que foi obtido consentimento), sendo que não devem ser recolhidas mais informações do que as necessárias aos fins a que se destinam.

Após terminar a atividade de tratamento, a prova do consentimento não deve ser conservada mais do que o necessário para o cumprimento de um dever legal ou para efeitos de declaração, exercício ou defesa de direitos num processo judicial[41].

[40] Nos termos do considerando 42) *ab initio* do RGPD.

[41] Em conformidade com as alíneas b) e e) do n.º 3 do art.º 17.º do RGPD – "(…) b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; e, e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial."

6.2. Retirada do consentimento

O Regulamento confere destaque à retirada do consentimento, prevendo que o responsável pelo tratamento deve garantir que "*o consentimento deve ser tão fácil de retirar quanto de dar*"[42] e a qualquer momento, e o facto de o consentimento ser retirado não compromete a licitude do tratamento de dados efetuado com base no consentimento anteriormente obtido.

Todavia, o responsável pelo tratamento tem a obrigatoriedade de informar o titular dos dados pessoais, aquando da obtenção do consentimento, da prerrogativa de poder vir a retirar o consentimento a qualquer momento.

7. Considerações finais

Desde a plena aplicabilidade do RGPD[43], os titulares dos dados pessoais têm, de facto, sido confrontados com inúmeros, diremos demasiados, pedidos de consentimento, muitos dos quais desnecessários e que refletem as dificuldades e dúvidas por parte dos responsáveis pelo tratamento; a este propósito, diga-se que, se o consentimento dado por uma pessoa antes do RGPD ser aplicável estiver em conformidade com as condições e os requisitos do regulamento, não é necessário ser solicitado de novo o consentimento[44] [45].

Só é necessário um novo consentimento se a organização obteve o consentimento dos seus clientes há alguns anos utilizando um sistema de opções pré-validadas *online*. Este modelo de obtenção de consentimento deixou de ser válido em 25 de maio de 2018 - logo, o responsável pelo tratamento terá de obter um novo consentimento, caso pretenda continuar a efetuar o tratamento dos dados.

Assim, cremos que a problemática na obtenção do consentimento residirá, essencialmente, na forma como o pedido é apresentado e formulado ao titular dos dados pessoais.

---

[42] Cfr. n.º 3 in fine do art.º 7.º do RGPD.
[43] *i.e.,* 25 de maio de 2018.
[44] Neste sentido veja-se as orientações do GRUPO DE TRABALHO DO ARTIGO 29.º. *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*. *Ob. Cit*. p. 34 a 35 – "Os responsáveis pelo tratamento que procedem atualmente ao tratamento de dados com base no consentimento em conformidade com as normas nacionais de proteção de dados não são automaticamente obrigados a renovar totalmente todas as relações de consentimento existentes com os titulares dos dados em preparação para o RGPD. O consentimento que foi obtido até à data continua válido na medida em que esteja em consonância com as condições do RGPD. É importante que, antes de 25 de maio de 2018, os responsáveis pelo tratamento revejam pormenorizadamente os processos de trabalho e registos atuais, para garantirem que os consentimentos existentes cumprem os critérios do RGPD. Na prática, o RGPD eleva o nível de exigência no que toca à aplicação de mecanismos de consentimento e introduz vários novos requisitos que exigem que os responsáveis pelo tratamento alterem os mecanismos de consentimento, em vez de apenas reescreverem as políticas de privacidade"
[45] Cfr. considerando 171) do RGPD.

Bibliografia

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA, de 7 de dezembro de 2000. **Jornal Oficial da União Europeia**. PT (30.3.2010).

DEODATO, Sérgio – **A Proteção dos Dados Pessoais de Saúde**. Lisboa: Universidade Católica, outubro de 2017. ISBN: 978-972-54-0578-9.

DIRETIVA Nº 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO, de 24 de outubro de 1995. **Jornal Oficial das Comunidades Europeias**. (23.11.95).

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE 2018 – **Handbook on European data protection law**. 2018 edition. Luxembourg: Publications Office of the European Union, 2018. ISBN : 978-92-871-9849-5.

GRUPO DE TRABALHO DO ARTIGO 29.º. **Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679.** [Em linha]. Adotadas em 28 de novembro de 2017. (Última redação revista e adotada em 10 de abril de 2018. [Consultado em 20 mai. 2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf

REBOLLO, Lucrecio – **Protección de datos en Europa: origen, evolución y regulación actual**. Madrid: Editorial Dykinson, 2018. ISBN: 978-849-14-8655-8.

REGULAMENTO (UE) Nº 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016. **Jornal Oficial da União Europeia**. PT (4.5.2016).

GDPR impact on organisations - Six months on

Maria Flores[1], CIPP/E

Summary

GDPR brings a very big change in data protection regulation that affects organisations in a very deep way. Accountability is key and it's very important to ensuring Data Subject Rights.

There needs to be a balance between the economic activity of the organisation and respect for privacy that already existed before this regulation. All the processes for the GDPR implementation must be scalable, sustainable and measurable, in order to keep track of the implementation of GDPR and take the necessary measures to improve whatever is necessary.

This paper explores how the GDPR has impacted organisations six months after the implementation in the UK.

GDPR has been the biggest regulatory change in compliance affecting every single organisation that processes personal data. What does it means in practice?

The new regulation has affected every organisation in a different way. A difference very easy to appreciate between more and less regulated sectors, like the finance sectors, which is already used to regulations and they have to juggle the implementation with other regulations like PSD2 or MIFID.

The first impact in organisations has been to implement the letter of a law that it goes beyond compliance. It's more than updating an online privacy policy. It requires mapping personal data processes, respond to requests from data subjects, implementing accountability mechanisms, managing contract with third parties, anticipating data breaches and cybersecurity obligations. The steps towards GDPR readiness will depend on the type of organisation, personal data collected, the GDPR footprint and exposure, the organisation's risk tolerance. There are many decisions organisation have to take regarding the following requirements:

[1] Law Degree (LLB / LLM equivalent): University of Salamanca (Spain) (2007). Data Protection Professional and an ISEB / BCS qualified multi-lingual Business Analyst.

- Identify which personal data that is processed and ensure is processed lawfully, fairly and transparently
- Create clear privacy notices that include information about the purposes of the data processing, the legal basis, categories of recipients, and data retention period for that data
- Respond to data subject requests: right to access, modify and restrict the processing of data, data portability and right to be forgotten
- Data mapping of all personal data-processing activities
- Appointment of a data protection officer and or an EU representative for the cases that is necessary
- Updating supplier contracts to include GDPR guarantees
- Notify breaches within 72 hours of being aware
- Adherence to rules and mechanisms regarding cross-border data transfers

Non-compliance with the GDPR can result in two levels of fines: the greater of €20m or 4 percent of global turnover, or €10m or 2 percent of global turnover, depending on the nature of violation.

However, the implementation of the above is not simple in itself. Re-negotiating contracts with third parties and discovering data can be challenging when the third parties are immersed in their own projects or there are legacy systems involved. Let alone if there's some sub-processing and this may be in a non EU country.

In the midst of all this work and in the way of the implementation work getting into business as usual, a new function, if it didn't exist before emerges: the privacy function, the function that will care for the privacy of activities and data subjects within the organisation.

To the challenges mentioned above, and in order to make the project work, GDPR needs to be implemented like a change management programme, so there's a real change that reaches every area of the organisation by aligning with the organisational strategy, culture and structure.

From the Change Management perspective and in order to achieve effective change, the organisation as a whole needs to be taken account and understand and address how change can affect people.

There are different sides in Change Management. One of them is how to write requirements or user stories in a way that incorporates the learning necessary from the business areas

Another side is to take into account how people react to change. Kubler-Ross wrote about the stages people go through when they receive tragic news as a coping mechanism.These are the stages individuals go through when dealing with change. These stages need to be managed. Otherwise, change won't work.

The SARAH model of change defines these stages. SARAH is an abbreviation for:

- Shock
- Anger
- Resistance
- Acceptance
- Healing/Hope

Understanding these phases helps stakeholders support the needs of the business users from inception of the project until implementation. The most critical phase is Resistance. It's crucial to support people by providing positive messages to get through resistance, work into acceptance and allow for permission in experimenting and failure as there's a new paradigm that needs to be explored and reach into Healing/Hope and find out the positive aspects of the new business reality.

Privacy teams after the implementation or readiness stage of GDPR keep on working on keeping on creating or building a privacy culture with awareness, training and workshops, privacy impact assessments, reviewing data mapping, assessing in privacy by design: the work never stops.

Accountability is key for this regulation to work. Fines and consequent reputation damage have made this regulation so relevant and key for the boards attention. A way to show accountability is by documenting decisions made.

The ICO, the British Data Protection Authority have been receiving complaints. In July, the ICO issued the first formal enforcement action against a Canadian data analytics firm requiring the firm to cease processing any personal data of UK or EU citizens obtained from UK political organisations. In other parts of Europe, data protection authorities in Germany and France announced that they would start audits

to check compliance with the GDPR. Other governments (200) like Israel or Brazil have moved on their own data privacy regulations to keep up with the GDPR regime.

California with their California Consumer Privacy Act provides GDPR-like protections and gives California consumers broader access and control over their personal information. From Jan. 1, 2020. There's a trend with GDPR-inspired data protection soon becoming the new normal.

Going Forward

This has been the last six months so far. But what does the future have in store? One of the main reasons for this regulation was technology. And technology will keep on moving and challenging our lives and regulations.

New Technologies

Blockchain

Blockchain is a database where data is stored and distributed to a large number of computers and where all entries: transactions, are visible to all users. A blockchain is not a data processing operation with its own purpose but a technology that can be used for many kinds of processing operations. Because Blockchain has been quite popular, it had been in the view of technologist and regulators for different reasons for a while. How can it be compliant with GDPR.

as it may be obscure in many ways and technologist would be saying that GDPR hadn't been thought for them.

The CNIL, the French Data Protection Authority has released a guidance on blockchain. The guidance begins with a simple premise: when a blockchain contains personal data, the GDPR is applicable.

1. Data controller and processor roles
   - the blockchain participants with rights to write on the chain and decide whether to send data for validation by miners, are data controllers.
   - Smart contract developers processing personal data on behalf of a participant and miners who validate transactions are data processors.
   - CNIL is still considering if miners in a public blockchain are data processors.

2. Risk minimisation

- When possible, use alternative solutions to blockchain that facilitate GDPR compliance.
- Use permission blockchains transfers of data outside of the EU.
- any additional personal data is not stored on the blockchain in cleartext format.

3. How can blockchain applications ensure data subject rights?

- The CNIL guidance indicates rights access and portability.
- While it is technically impossible to grant requests for erasure of personal data registered on a blockchain, use of cryptological solutions can make such data practically inaccessible and closer to the goal of ensuring the right of erasure.

Artificial Intelligence

Artificial Intelligence ie, AI, ie, the algorithm is something that is much closer to us, in every profiling and every automation of systems. And we are getting more and more of it. It's already regulated in the current legislation. The impact on individual rights could be massive. Decisions cannot be left alone to the machine.

When working with AI, there's the risks of allowing an algorithm to decide certain people's lives and getting too much information about certain groups of individuals and not about others. AI can be used as a tool to solve a problem. A problem that is not reviewed and it's not considered to be solved in another way. Therefore, when with artificial intelligence it is important to be transparent, ensure that the customers understand the privacy policy and obtain permission to do so. In order to help manage privacy compliance, companies should (t) keep a clear record of how their AI will collect, store, use and share data and in coordination with legal counsel determine how this information should be disclosed.

References:

Franklin, M (2018). *Integrating project and change management.* Retrieved from https://www.linkedin.com/pulse/integrating-project-change-management-melanie-franklin/

Managing Change: SARAH Model of Change. Retrieved from https://businessanalystlearnings.com/ba-techniques/2016/4/3/managing-change-sarah-model-of-change

Figliolino, V (2016). *Change Management: Sarah model.* Retrieved from https://leansixsigma.community/blog/view/12394/change-management-sarah-model

Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data (2018). Retrieved from https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

Big data, artificial intelligence, machine learning and data protection (2017). Retrieved from https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Lee, P (2017). *Let's sort out this profiling and consent debate once and for all.* Retrieved from https://privacylawblog.fieldfisher.com/2017/let-s-sort-out-this-profiling-and-consent-debate-once-and-for-all

A importância da segurança dos dados na internet

Mário Antunes, ESTG-IPLeiria

Resumo

A Internet é uma infraestrutura de comunicações à escala global, que interliga um enorme e crescente número instituições, equipamentos e de utilizadores. Os serviços suportados pela Internet, onde se destaca a *World Wide Web* (WWW)[1], envolvem a comunicação entre aplicações e transportam dados dos utilizadores, empresas e instituições. A utilização em massa da Internet e a crescente importância (e valor) dos dados aí transportados tem evidenciado várias fragilidades da Internet ao nível da segurança e privacidade dos utilizadores. Tal é patente no crescente aumento de ciberataques que têm provocado danos avultados nos utilizadores e empresas.

Nesta comunicação evidenciam-se os principais aspetos relacionados com a importância dos dados e apresentam-se os principais tipos de ciberataques, apontando-se sinteticamente as principais medidas para a sua mitigação. Atendendo a que as principais ameaças advêm da manipulação dos cidadãos e empresas, por exemplo através de engenharia social, esta comunicação pretende alertar para a consciencialização daqueles sobre a importância dos dados e a necessidade de adotar estratégias defensivas na utilização dos serviços da Internet.

1. A comunicação na Internet

A Internet é uma infraestrutura de comunicações à escala global. Integra o ciberespaço e interliga um vasto conjunto de instituições, equipamentos e utilizadores.

Genericamente, a Internet tem um funcionamento muito simples e assenta em princípios de comunicação básicos, que originalmente não teve preocupações com a segurança entre os extremos comunicantes (aplicações e utilizadores).

A comunicação na Internet faz-se através de aplicações que são manuseadas por utilizadores. Essas aplicações estão em execução num equipamento informático (por exemplo um computador pessoal ou um *smartphone*) e comunicam através de troca de mensagens protocolares simples e em formato de texto. Pode afirmar-se que a comunicação na Internet é, em larga medida, do tipo “cliente/servidor” e funciona através de um paradigma de comunicação do tipo “pedido/resposta”.

[1] Será utilizada a designação “web” ao longo do texto.

Ou seja, tomando como exemplo o serviço *web*, a comunicação assenta em duas aplicações principais: um cliente implementado maioritariamente por um *browser* (Google Chrome ou Internet Explorer), que efetua pedidos a um servidor *web*. Este processa o pedido recebido e responde ao cliente com o recurso solicitado, que pode ser por exemplo uma página HTML[2]. As mensagens protocolares que implementam o desenho do protocolo em causa (no caso do serviço *web* o protocolo é o HTTP[3]), são trocadas entre o cliente e o servidor são textuais e constituídas por informação relevante para que as aplicações processem da melhor forma os pedidos e respostas. Esta informação é adicionada à mensagem original sob a forma de "cabeçalhos"[4], em texto não cifrado e potencialmente acessível por qualquer pessoa através de uma aplicação de recolha de tráfego na rede.

Há imensos protocolos aplicacionais que desempenham várias funções e implementados por aplicações específicas. Além do serviço *web*, implementado pelo protocolo HTTP, podemos igualmente destacar o serviço de gestão de nomes implementado pelo protocolo DNS ou o serviço de processamento de email, que têm três protocolos principais: SMTP, POP3 e IMAP.

Além do facto dos protocolos aplicacionais assentarem em mensagens textuais, também não foram originalmente desenhados para garantirem confidencialidade dos dados que transportam. Por exemplo, no desenho da Internet e dos protocolos aplicacionais não foi tido em conta a implementação de mecanismos de cifragem ponto-a-ponto entre as aplicações. Com o aumento do tráfego na Internet e as preocupações crescentes em garantir a confidencialidade dos dados aí transportados, surgiram as versões "seguras" dos protocolos aplicacionais. Nesse sentido, surgiu o protocolo HTTPS que oculta os dados transportados no serviço *web* através de mecanismos de cifragem entre as aplicações. Outros protocolos tiveram a sua versão segura, como por exemplo no serviço de email com a implementação dos protocolos SMTPS, POP3S e IMAPS.

2. A *cloud*

O modo de utilização da Internet e dos seus serviços foi mudando ao longo do tempo. Se no início a motivação dos utilizadores era descarregar (*download*) recursos alojados por exemplo em servidores *web*, atualmente os utilizadores são também

[2] Linguagem de *markup* que representa graficamente num *browser* os efeitos de hipertexto
[3] Hyper-Text Transport Protocol. Atualmente a versão segura é cada vez mais utilizada (HTTPS).
[4] *Headers* na designação anglo-saxónica.

produtores de conteúdos e as ações que desempenham são maioritariamente de *upload*. Veja-se por exemplo a atividade das redes sociais, onde os seus utilizadores aproveitam as potencialidades deste tipo de aplicações para criar uma rede virtual de contactos, com quem possam partilhar conteúdos variados e publicar estados. Também do ponto de vista da privacidade e confidencialidade, são vários os desafios que se colocam à partilha de dados, por vezes confidencias, nas redes sociais. Uma das razões principais é o facto de os dados destas aplicações estarem alojados na *cloud.*

A *cloud* é um espaço de armazenamento e computação gerido por um "operador de *cloud".* As vantagens da sua utilização são evidentes, realçando-se o facto de as empresas não terem necessidade de instalar uma infraestrutura própria, podendo colocar os seus dados e as suas unidades de processamento (tipicamente máquinas virtuais) em infraestruturas específicas para o efeito. As *clouds* podem ser públicas, privadas ou híbridas, dependendo fundamentalmente do caráter proprietário da infraestrutura, o que tem implicações diretas no nível de segurança dos dados que aí são armazenados. Por exemplo, a *cloud* das empresas Amazon (Amazon Web Services - AWS), da Microsoft (Azure) ou Google são exemplos de *clouds* públicas onde são alojados os dados de várias empresas e utilizadores. Por outro lado, algumas empresas (normalmente de média/grande dimensão) pode instalar uma infraestrutura de *cloud* privada, onde apenas residem os seus dados. Os modelos híbridos de *cloud* integram uma solução baseada nos dois modelos anteriores. No caso concreto das redes sociais, como o Facebook, os dados dos utilizadores são alojados num serviço de *cloud* gerido pela Facebook, mas onde estão alojados dados de muitos (milhares de milhões) de outros utilizadores e empresas. Do ponto de vista de segurança dos dados, é importante ter em conta que, embora haja uma sensação de segurança (por exemplo, supostamente apenas partilhamos as imagens e os vídeos com a nossa rede de contactos), na prática o tipo de conteúdos (essencialmente multimédia) pode convidar à sua utilização indevida e até mesmo à sua exfiltração.

3. Direito de admissão na Internet

Ao contrário de outros serviços que utilizamos no dia-a-dia, em que o uso abusivo e a prevaricação são punidos com a inacessibilidade ao serviço, na Internet esse não é o caso. No desenho da Internet e nos seus princípios fundamentais, está consagrado o acesso livre a todos os utilizadores. Ou seja, embora seja evidente nos

dias de hoje que há utilizadores que têm um uso abusivo da Internet e que aí cometem crimes, não há possibilidade de lhes impedir o acesso. Se tal possibilidade houvesse, a de impedir o acesso aos serviços da Internet pelos utilizadores prevaricadores, de pouco serviria, já que estes recorrem à "*web* não regulada", designada por *deep web*. Neste espaço a atividade é anonimizada, o tráfego gerado é cifrado e o crime tem condições favoráveis para proliferar.

4. Sobre o valor dos dados na Internet

Uma consulta ao *Cambridge Dictionary*[5] leva-nos a duas definições genéricas do termo "dado"[6], designadamente: 1) "*facts or numbers collected to be examined and considered and used to help decision-making"* e 2) *"information in an electronic form that can be stored and used by a computer"*. Esta última definição é mais atual e comporta a realidade da Internet e do formato digital dos dados que aí circulam.

A massificação da utilização da Internet e a total dependência pelos meios de comunicações digitais para transportar dados do negócio, tem levado a um aumento exponencial do valor destes, tornando por isso apetecível a sua exfiltração e roubo.

É atualmente fácil aceitar a Google, Apple, Facebook e Amazon[7] como as maiores empresas da Internet, em termos de volume de dados que gerem, tanto de utilizadores como de empresas. Este quarteto, a que se adiciona a Microsoft, por si só gere os dados pessoais e sensíveis de muito milhões de utilizadores, como sejam: informação sobre cartões de crédito, correio eletrónico e conteúdos multimédia guardados com sendo de acesso restrito, apenas para mencionar alguns. Sendo estes dados confidenciais e ao mesmo tempo sensíveis e transacionáveis, o seu valor é elevado e a sua perda poderá implicar elevados dados pessoais e empresariais.

Por esse motivo, a questão que se deve colocar é se os indivíduos e as empresas têm uma contabilização do valor real dos dados. Ou seja, quanto é que uma empresa (ou cada um dos de nós) perde na eventualidade dos seus dados serem roubados ou apagados. E as perdas não são apenas monetárias, já que há custos que poderão ser de difícil contabilização, como a perda de credibilidade ou a publicidade negativa.

[5] https://dictionary.cambridge.org/
[6] *Data*, na definição anglo-saxónica
[7] Também designado por GAFA

5. Ciberataques e medidas de mitigação

O termo “ciberataque” refere-se a ataques que ocorrem no ciberespaço. Os ataques podem ser classificados através de vários critérios, desde a motivação, a abrangência (internos, externos), o nível de intrusão (passivos, ativos) e o grau de impacto que pode provocar nas vítimas. Nesta secção elencam-se os mais relevantes e que estão relacionados diretamente com o roubo de dados, remetendo-se para outras referências uma análise mais detalhada desta matéria[8].

O **phishing** é uma técnica que consiste em tentar confundir os utilizadores da Internet (por exemplo do serviço *web*), para que forneçam informações confidenciais, como credenciais para aceder a determinado *site* ou o número do cartão de crédito.

Estas tentativas são normalmente efetuadas através do envio de emails ou de mensagens instantâneas (por exemplo via SMS), através de remetentes aparentemente legítimos, que são combinadas com mecanismos de redireccionamento para páginas *web* fraudulentas onde é feito o pedido das informações confidenciais.

Estas técnicas são variadas e têm sido aperfeiçoadas ao longo do tempo, no sentido de diminuir, ou até mesmo eliminar, a estranheza da vítima quando recebe uma mensagem a pedir informação confidencial. O objetivo é sempre que a vítima acredite de facto que o remetente é fidedigno e que o email recebido é legítimo e que não levanta suspeitas.

Um exemplo concreto consiste no envio de mensagens de email falsas, em nome de bancos. Neste caso os utilizadores são convidados a aceder a um *link web* falso, através de um endereço de URL forjado, onde são efetuadas solicitações fraudulentas, como o pedido das credenciais de acesso à conta bancária.

Estas páginas fraudulentas poderão ser muito parecidas com as originais, o que poderá eludir facilmente os utilizadores menos experientes e com menos conhecimentos sobre o funcionamento da Internet.

Há algumas burlas conhecidas que tiveram por base ataques de *phishing*, onde a motivação consistiu em obter informações privilegiadas das vítimas:

- As bem conhecidas “cartas da Nigéria”, em que o remetente é um burlão que conta uma história bem encenada sobre a existência de um negócio milionário para o qual necessita de ajuda da vítima. Neste caso o negócio não existe e o

[8] Mário Antunes, Baltazar Rodrigues; *"Introdução à Cibersegurança - a Internet, os aspetos legais e a análise digital forense"*; 1ª edição; Abril 2018; ISBN: 978-972-722-861-4; Editor: FCA

objetivo do burlão é obter dados pessoais das vítimas para que possa cometer outros crimes com identificação falsa.

- Falsas “empresas de recrutamento” que solicitam o envio por email de informações pessoais, como o nome, morada e contacto de telemóvel. Esta última informação permitirá iniciar posteriormente a recolha de dados do telemóvel em causa, como fotos, contactos, SMS, entre outros.
- Angariação de “agentes financeiros” que sirvam de intermediários na transferência de dinheiro para uma conta bancária. Estes utilizadores são vulgarmente denominados por *money mule* e são normalmente “contratados” através de mensagens de *email* destinadas para esse fim. O dinheiro que é transferido por esta via resulta normalmente de atividades ilícitas.

Há vários cuidados e medidas que poderão ser tomadas para mitigar os ataques de *phishing*, designadamente:

- Não abrir ficheiros que estejam em anexo nos emails ou seguir URL que se encontrem em mensagens das quais os remetentes sejam desconhecidos. É normalmente nos ficheiros em anexo ou nos endereços URL que será efetuado o *phishing* dos dados confidenciais.
- Por norma as entidades comerciais não solicitam informações confidenciais por email. Por exemplo, os bancos não pedem informação sobre os PIN de cartões bancários ou uma sequência de dígitos do cartão matriz.
- Em transações onde seja necessário enviar informações confidenciais, como por exemplo uma compra com cartão de crédito, deve certificar-se que o *site* é seguro e fidedigno.

Os ataques do tipo ***ransomware*** consistem no acesso ilícito a um computador através da instalação de um vírus ou programa malicioso, seguindo-se a posterior encriptação dos dados aí armazenados. De seguida os atacantes iniciam a fase de extorsão, exigindo quantias em dinheiro para que os dados fiquem novamente acessíveis.

O termo ***sextortion*** refere-se a um tipo específico de extorsão cujo objetivo consiste em extorquir favores sexuais à vítima, recorrendo para tal à ameaça de divulgação de imagens comprometedoras ou informações sexuais. As fotos e vídeos comprometedores estão normalmente alojados nas redes sociais e a ameaça utilizada é a sua partilha por outros utilizadores.

A técnica de ***carding*** consiste na manipulação e obtenção de dados pessoais armazenados nas bandas magnéticas dos cartões de crédito. Há vários métodos que

são utilizados para a recolha dos dados, como seja a instalação de leitores falsos nos equipamentos utilizados para leitura de cartões (por exemplo, caixas ATM e POS). Os ataques utilizam normalmente estas técnicas em conjunto com outras que pretendem obter o PIN do cartão. Entre as várias técnicas podemos indicar a utilização de micro-câmaras ou de teclados falsos instalados nas caixas ATM.

A evolução recente dos ciberataques, quanto aos alvos, *modus operandi* e motivação, releva que a expectativa é que sejam cada vez mais sofisticados, tornando mais complicada a sua deteção e mitigação. O recurso a mecanismos de encriptação e anonimização (por exemplo através do uso de VPN e da rede TOR) torna cada vez mais complexa a tarefa de identificar os ataques, após a ocorrência de um ataque. O uso da *cloud* para distribuição dos ataques é uma tendência que deverá continuar. Os serviços de *malware* na cloud (*malware as a service*) é atualmente uma realidade na utilização de ataques distribuídos à escala global (por exemplo ataques de negação de serviço[9]). Por fim, o impacto dos ataques é cada vez mais elevado, nomeadamente em perdas materiais. Os dados têm um valor cada vez maior e a sua perda provoca um impacto negativo cada vez maior. Além dos perdas materiais referidas anteriormente, há ainda a acrescentar o impacto psicológico (por exemplo em ataques de *sexting* ou de *ransomware*) que os ciberataques têm nas vítimas, quer sejam empresas ou indivíduos.

6. Conclusões

Nesta comunicação abordámos sucintamente o funcionamento genérico da Internet, dos seus serviços principais e da *cloud*, tentando justificar a razão de existirem vulnerabilidades. De seguida definimos “dados” e destacámos a necessidade de quantificar o seu valor. Definimos ainda ciberataques e identificámos alguns que lidam diretamente com os dados dos utilizadores. Para cada um apresentámos algumas medidas de mitigação.

A consciencialização para o uso responsável da Internet é de central importância. Se, por um lado, todos os utilizadores (individuais, empresas e organizações) poderão ser alvo de ataques (físicos e lógicos), por outro lado alguns desses ataques poderão ser mitigados pela adoção de cuidados simples que devem fazer parte da utilização consciente da Internet. Portanto, a primeira conclusão reside

[9] *Denial of Service* (DoS) na denominação anglo-saxónica.

na necessidade de sensibilizar os utilizadores para as principais ameaças existentes na Internet e para as correspondentes medidas de mitigação que se podem usar.

A utilização de soluções tecnológicas robustas deve nortear a aquisição de equipamentos e de sistemas de informação. Por vezes a aquisição de um equipamento mais barato, como por exemplo um *smartphone*, poderá sair caro se a marca não disponibilizar atualizações frequentes de segurança.

É fundamental gerir eficientemente a pegada digital. A produção de conteúdos e o seu alojamento na *cloud* pode proporcionar condições favoráveis para ciberataques que poderão provocar danos graves nos utilizadores e nas empresas. Merece destaque neste domínio a publicação e gestão de conteúdos efetuada nas redes socias.

Por fim, mas não menos importante, deverá haver uma aposta na formação e educação contínua dos utilizadores ao nível da utilização da Internet e das tecnologias de informação e comunicação em geral. Uma boa parte dos ciberataques poderia ser evitada, já que se baseia na engenharia social e no comportamento dos utilizadores. Nesse domínio, a formação e educação dos utilizadores irá coloca-los em alerta para cenários típicos de ataque, evitando antecipadamente eventuais perdas e danos que os mesmos possam causar.

Painel II – O RGPD no setor Público

Impacto nas Autarquias Locais, medido pelo acolhimento global

Rajani Oliveira[1]

Introdução

Legislar, ato de soberania de um **País**[2], cuja organização interna se estrutura juridicamente num **Estado de direito**, visa sempre um determinado objetivo, em regra a prossecução do bem comum, sendo este, a proteção dos interesses da **Nação**[3], corporizada pelo **Povo**[4], seu substrato pessoal e humano, repousando no estatuto de **Cidadania**, os seus direitos e obrigações, em regra residentes na sua **Mátria**[5], ou seja, a sua terra de nascimento, ligados pelo cimento da língua – vulgo a **Pátria**[6] – esta já não só adentro de fronteiras, as mais antigas do mundo ocidental desde pelo menos o século XI, mas extramuros, porque na diáspora dos falantes por esse planeta fora.

O Poder Local tem, neste sistema vivencial, secular, em Portugal, uma particular importância, e uma não menor responsabilidade, pois foi sob a sua égide que os nossos primeiros governantes e legisladores, assentaram a sua ação administrativa, já então, para combater o desmesurado poder de alguns, nobreza e clero, o que lhes valeu a integração nas cortes, em representação do chamado "*terceiro estado*" o Povo, através de representantes das comunidades com as suas "súplicas".

O advento da adesão à então CEE, hoje metamorfoseada em União Europeia, ao longo das últimas décadas, trouxe novas realidades legislativas … se pensarmos que em todo o seu Reinado Dom Afonso Henriques produziu pouco mais que 600 diplomas, e foi dos reinados mais longos em Portugal, comparado com a profusão legislativa nacional, numa base mensal, à qual se

---

[1] Mestre em Políticas Regionais da União Europeia, pela Universidade Complutense de Madrid, Cátedra "*Jean Monet*"; Pós-Graduado em Gestão avançada de Recursos Humanos, pela Universidade Independente; Pós-graduado em Comunicação e Marketing Político, pela Universidade Independente/Complutense de Madrid; Licenciado em Administração Regional e Autárquica, pela Universidade Independente; Investigador e Vice-Presidente na Associação Portuguesa de Administração e Políticas Públicas; Autor de diversas comunicações a fóruns nacionais e internacionais; Formador e Consultor nos domínios da Administração Pública, e gestão privada.

[2] Dias, José António Rajani Oliveira, "O Poder Local nas Constituições Portuguesas", Editora Artelogy, 2016.

[3] *Idem*.

[4] *Idem*.

[5] *Idem*.

[6] *Idem*.

juntam as diretivas comunitárias e os regulamentos comunitários, estamos perante uma mudança de paradigma abismal.

Este enquadramento tem o propósito de chamar à atenção da enorme importância do Poder Local, no acolhimento, e cumprimento escrupuloso das regras que afetam diretamente o **substrato pessoal das autarquias**, compostos pelos seus Municípios e Freguesias, colocando no ombro dos representantes destes, os respetivos eleitos locais, a enorme responsabilidade de não se furtarem ao cumprimento de um Regulamento Comunitário – leia-se o RGPD -, a cuja aplicação estão diretamente vinculados, ao contrário das diretivas comunitárias que carecem de transposição nacional.

Num programa da RTP3, sobre Cybersegurança e RGPD, transmitido em direto, o autor teve a oportunidade de colocar uma questão à senhora Presidente da Comissão Nacional de Proteção de Dados, a saber: “Quantas autarquias comunicaram já, para efeitos de registo na CNPD, os respetivos Delegados de Proteção de Dados?”, sendo certo que sobre as autarquias impendem a obrigação de nomear esse responsável e comunica-lo à CNPD.

Pese embora esse dado não estivesse na posse da senhora Presidente da CNPD, naquela oportunidade, posteriormente foi-me gentilmente fornecida essa informação: **11** Municípios e **3** Freguesias, à data de **21 de Agosto de 2018**, cumpriram com essa obrigação legal.

O Regulamento Geral de Proteção de Dados, foi aprovado em 2016, e teve um “*vacatio legis*” de 2 anos, entrando em vigor efetivo a 25 de maio de 2018, a fim de permitir uma adequada preparação dos seus destinatários, e já se sabia que a administração pública estaria obrigada à nomeação de um responsável de proteção de dados (EPD). Ainda assim, o Poder Local português ignorou esses 2 anos, e desde a entrada em vigor até agora, decorreram 6 meses, mesmo admitindo que entretanto aquele número fornecido pela CNPD possa ter registado algum incremento, fica muito longe do universo de 308 Municípios, e mais de 3.000 Freguesias.

Assim o impacto, em termos de acolhimento, nas autarquias locais do RGPD, cifra-se numa percentagem de 0,03%, no que respeita aos municípios, e de 0,001no que respeita às freguesias.

Talvez se faça alguma luz atentando o complexo e obsoleto modelo administrativo e gestional, com que as autarquias e seus responsáveis se confrontam, na defesa de quem é a sua razão de ser – o Cidadão.

A aplicação do RGPD, nas autarquias locais, tem de se compaginar com conceitos e institutos jurídicos específicos deste patamar da administração pública do Estado Português, sejam eles – a Descentralização, Desconcentração e a Deslocalização (cada um deles com as suas peculiaridades) conjugados com as Atribuições das autarquias e dos Poderes e Competências dos seus órgãos (executivos individuais e colegiais, e os deliberativos colegiais), através dos institutos jurídicos da Devolução de Poderes, e da Delegação de Poderes e competências (não se confundindo com a delegação de tarefas).

Para além disso, importa ter presente que as Autarquias Locais, têm de conjugar as obrigações decorrentes do RGPD, com as posições da CADA (Comissão de Acesso aos Documentos Administrativos) e a CNPD (Comissão Nacional de Proteção de Dados), sem perder de vista o CPA (Código do Procedimento Administrativo).

É, enfim esta a "malha" com que as autarquias locais têm de se debater, e estar em conformidade… uma realidade bem diversa daquela outra de uma qualquer empresa do sector privado, em virtude da qual se pretende, sucinta, mas objetivamente explicar, no nosso trabalho.

1. A evolução da Proteção de Dados – sinopse

1.1. Na Europa

As preocupações com a proteção de dados pessoais, tornaram-se efetivas, com a Convenção dos Direitos do Homem (1950)[7], genericamente preocupada com a defesa da dignidade humana, e afins, reforçada e reiterada com o tratado do Conselho Europeu, conhecido como : A Convenção 108 do Conselho da Europa (1981)[8], que se realizou em 28 de janeiro de 1981[9], tendo sido, em termos internacionais, o primeiro instrumento a regular a proteção dos

[7] https://www.echr.coe.int/Documents/Convention_POR.pdf
[8] file:///C:/Users/asses/Desktop/RGPD/Convenção%20108%20Conselho.pdf
[9] Esta data passou a ser celebrada como o dia internacional da proteção de dados, assinalada todos os anos, sendo a próxima celebração, em 2019, a 38ª.

dados pessoais, de forma especifica, visando "garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal", na esteira do que já, em termos muito genéricos, se assegurava na Convenção Europeia dos Direitos do Homem (CEDH) , concretamente no seu artigo 8º, de 4 de novembro de 1950, onde se consagra o direito ao respeito pela vida privada e familiar "*Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo domicílio e pela sua correspondência*" .

Em 1995, a Diretiva da UE relativa à proteção de dados pessoais[10] visava proteger os direitos e liberdades fundamentais das pessoas singulares, tendo sido complementada com outros diplomas legislativos, mormente a Diretiva relativa à privacidade eletrónica, para o sector das comunicações.

O direito à proteção dos dados pessoais é expressamente reconhecido no artigo 8.° da Carta dos Direitos Fundamentais da UE[11] e no Tratado de Lisboa[12], no qual a Carta está integrada. O artigo 16.º (do Tratado sobre o Funcionamento da União Europeia - TFUE) fornece a base jurídica para as normas de proteção de dados aplicáveis a todas as atividades abrangidas pelo direito da UE.

1.2. Em Portugal

O regime democrático[13], acolhe preocupações com o cidadão, e neste particular com os direitos de personalidade, atinentes à proteção da sua privacidade, inscrevendo no texto constitucional de 1976, designadamente no seu artigo 35º[14], o qual viria a ser objeto de aperfeiçoamento na 1ª revisão

[10] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[11] Em especial os Artigos 7º e 8º reconhecem o respeito pela vida privada e a proteção dos dados pessoais como direitos fundamentais estreitamente relacionados, mas distintos.
[12] O tratado de Lisboa acabou com o sistema assente em pilares, e a proteção de dados ganhou uma base mais consistente, para a sua legislação, tendo este tratado criado novos poderes para o Parlamento Europeu que se converteu em colegislador juntamente com o Conselho e a Comissão.
[13] Consagrado em Portugal, em 25 de abril de 1974, no que ficou conhecido como "Revolução dos Cravos"
[14] Constituído apenas por 3 números: "ARTIGO 35.º (Utilização da informática) **1.** Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização. **2.** A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de

constitucional, em 1982[15], depois de uma iniciativa na Assembleia da República não ter tido sucesso, para verter em lei ordinária[16], a mesma matéria

Como consequência desta revisão constitucional, em especial por força do disposto no seu número 4, do artigo 35º, onde se prescreve que o conceito de dados pessoais deveria ser concretizado em lei ordinária, que haveria de conduzir a um conjunto de iniciativas legislativas, vertidas em 3[17] Projetos de Lei[18], e 4[19] Propostas de Lei[20], mas sem que nenhum deles tivesse logrado converter-se em Lei, por motivos diversos que não cabe, nesta sede escrutinar, antes registando-se uma efetiva vontade do legislador, quer ordinário, quer constitucional, em tratar uma matéria considerada de grande importância, ao ponto de ser acolhida na sede constitucional.

Apesar disso, as iniciativas legislativas conducentes à concretização do comando constitucional do nº 4, do artigo 35º, terminam em 1987, sem que se tivesse obtido ganho de causa par a definição de dados pessoais.

O impasse, ao nível dos órgãos de soberania legislativos[21], conheceria desenvolvimentos importantes, através do Provedor de Justiça[22], que requereu[23] ao Tribunal Constitucional[24] se pronunciasse pela existência de uma inconstitucionalidade por omissão, o que se veio a concretizar pelo acórdão do Tribunal Constitucional nº 182, de 1989[25].

---

dados não identificáveis para fins estatísticos. **3.** É proibida a atribuição de um número nacional único aos cidadãos."

[15] O termo "mecanográfico" foi substituído por "informático", e aditaram-se 2 novos números, a saber, um novo nº 2 (passando o texto do original a nº 3) com a seguinte redação "são proibidos os acessos de terceiros a ficheiros com dados pessoais e a respetiva interconexão, bem como os fluxos de dados transfronteiriços previstos na lei"; o remunerado nº 3 passa a ter a seguinte redação "a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se trate de dados estatísticos não individualmente identificáveis", e é aditado o nº 4 com a seguinte redação" a lei define o conceito de dados pessoais para efeito de registo informático"; o antigo nº 3 é renumerado para nº5.

[16] Projeto de Lei nº 214/I (criação do conselho de defesa da privacidade), de 22 de fevereiro de 1979.

[17] 1981, 1983, e 1987.

[18] Os Projetos de Lei são de iniciativa da Assembleia da República.

[19] 1982, 1984, 1984, e 1984.

[20] As Propostas de Lei são de iniciativa do Governo, sob autorização da Assembleia da República.

[21] Assembleia da República e Governo

[22] Órgão de Estado, cujos pareceres não são vinculativos.

[23] Em 13 de agosto de 1987.

[24] Órgão de Soberania.

[25] https://dre.pt/web/guest/pesquisa-avancada/-/asearch/612862/details/maximized?emissor=Tribunal+Constitucional&types=JURISPRUDENCIA&search=Pesquisar

Com isto os órgãos de soberania legislativos, tiveram mesmo de se empenhar a fundo e dois anos depois surge então a primeira lei ordinária, sobre esta matéria, pela mão da Assembleia da República, com a Lei 10/91.

A Lei 10/91, de 29 de abril, para além de se instituir o quadro normativo sobre a proteção de dados pessoais face à informática, cria a Comissão Nacional de Proteção de Dados Pessoais informatizados (CNPDPI).

Mais tarde, sentiu-se a necessidade de proceder a um reforço legislativo, o que se concretizou, através da lei 28/94, de 29 de agosto.

Posteriormente, o regime seria burilado com a Lei 67/98, de 26 de outubro (LPDP), que concretizou a transposição para o nosso ordenamento jurídico da Diretiva 95/46/CE, mais abrangente, e não apenas confinada aos dados informatizados, revogando a Lei 10/91 e a Lei 28/94. A CNPDPI, passa a CNPD (Comissão nacional de Proteção de Dados).

Também se assiste à publicação da lei 69/98 de 20 de Outubro, que regula o tratamento dos dados pessoais e a proteção da privacidade no sector das telecomunicações (transpondo a Diretiva n.º 97/66/CE, do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997).

A Lei 41/2004, de 18 de agosto (Proteção de dados Pessoais e privacidade nas telecomunicações)[26], viria a revogar a Lei 69/98.

Esta, por sua vez, haveria de ser revogada pela Lei n.º 46/2012, de 29 de agosto de 2012, procedendo à transposição da Diretiva n.º 2009/136/CE, do Parlamento Europeu e do Conselho, de 12 de julho, naquilo que foi a primeira alteração à Lei n.º 41/2004 de 18 de agosto, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, reforçando significativamente os direitos dos particulares quanto à proteção de dados pessoais.

Em 2018, a partir do dia 25 de maio, o Regulamento Geral da Proteção de Dados[27], do Parlamento Europeu e do Conselho (UE 2016/6979)[28], derrogam aquela legislação, até que, se promulgue um diploma nacional regulando o

[26] Transpôs para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas

[27] Os Regulamentos são de aplicação, geral, universal, automática em todos os estados-membros, e de forma completa, isto é, não pode ser aplicado de forma parcial.

[28] Publicado em 2016, mas efetivando-se em 2018.

quadro de sanções a aplicar, altura em que se efetivará, então, a revogação da Lei 41/2004, pois até lá continuará em vigor em tudo quanto não contrarie o RGPD, designadamente quanto a matéria de sanções a aplicar, quer por força dos diplomas em vias de serem revogados, quer por força do diploma geral das contraordenações[29], não havendo assim, para infelicidade de alguns, nenhum vazio legal, quanto a matéria sancionatória.

1.3. O Diploma - Regulamento Geral de Proteção de Dados (RGPD)

Os atos legislativos da União Europeia podem caracterizar-se, de uma forma simples, em número de cinco[30], sendo os mais importantes, porque vinculativos[31], os regulamentos comunitários, diretivas comunitárias, e decisões[32], os primeiros com origem no Parlamento Europeu e no Conselho, cuja aplicação em todos os estados-membros é direta, não carecendo de qualquer intervenção dos parlamentos nacionais, e os segundos com a mesma origem, estes já com necessidade de transposição para os ordenamentos jurídicos de cada estado-membro, através de ato legislativo dos respetivos parlamentos.

O Regulamento Geral da Proteção de Dados[33], do Parlamento Europeu e do Conselho (UE 2016/6979)[34], relativo à proteção dos dados pessoais das pessoas singulares, objeto de tratamento por terceiros, bem assim como à livre circulação desses dados mais conhecido como RGPD, é, pois, de aplicação direta[35], pese embora, o legislador da União Europeia, tivesse delegado, em sede do próprio regulamento, a necessidade de cada estado-membro proceder, através dos respetivos parlamentos, à adaptação, mitigada, é certo, da parte sancionatória[36], decorrente da violação deste normativo, por parte dos

[29] Decreto-Lei nº 433/82, de 27 de outubro.
[30] Os atos legislativos da União Europeia fixados pelo Tratado de Funcionamento da União Europeia, através do seu artigo 288º, visando a aplicação do Tratado de Lisboa, distribuindo por: Regulamentos, Diretivas, Decisões, Recomendações e Pareceres.
[31] Os atos legislativos juridicamente vinculativos são 3: Regulamentos, Diretivas e Decisões.
[32] As Decisões podem ser dirigidas especificamente a um destinatário, um estado-membro, empresas ou particulares.
[33] Os Regulamentos são de aplicação, geral, universal, automática em todos os estados-membros, e de forma completa, isto é, não pode ser aplicado de forma parcial.
[34] Que revoga a Diretiva 95/46/CE
[35] Significa que qualquer cidadão de um estado-membro pode invocá-lo diretamente sem necessidade de recorrer a tribunais.
[36] Até à concretização dessa parte, continua em vigor a Lei 67/98, no que se refere às coimas a aplicar.

destinatários prevaricadores, por via da aplicação de coimas[37], e não de multas[38], para além da adaptação orgânica que se impõe, e visa sobretudo a proteção de dados de pessoas singulares[39], vivas[40].

Para além deste Regulamento, foi igualmente aprovado, na mesma data, a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, não as do perímetro normativo do RGPD, mas as respeitantes ao tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados[41].

Sucede ainda, que este regulamento (RGPD) foi aprovado em 2016, mas com uma "*vacatio legis*"[42] de 2 anos, isto é, a eficácia do regulamento apenas se concretizou em 25 de maio de 2018, tendo-se considerado ser suficiente este período para a preparação e adaptação, ao novo normativo, por parte do universo de destinatários.

A circunstância, de cada estado-membro, ter a sua própria dinâmica, nesta transposição, ou seja, na fixação do sistema de coimas[43] e adaptação orgânica, em linha com os respetivos ordenamentos jurídicos internos, pode levar diferentes velocidades, de estado-membro para estado-membro, implicando, necessariamente, que nuns as coisas aconteçam com mais celeridade do que noutros.

[37] Valor pecuniário a pagar em caso de ilícito contraordenacional.
[38] Valor pecuniário a pagar em caso de ilícito criminal.
[39] Por maioria de razão exclui às pessoas coletivas (públicas ou privadas), incluso as sociedades comerciais unipessoais.
[40] Veremos mais á frente que o RGPD constitui-se como direito de personalidade, sendo que este, ao contrário do RGPD, também se aplica a falecidos.
[41] Revoga a Decisão-Quadro 2008/977/JAI do Conselho.
[42] Período durante o qual a Lei tem validade, mas não tem eficácia, não produz os seus efeitos.
[43] Em Portugal está plasmado no quadro do regime das contraordenações – DL. 433/82, de 27 de Outubro, e que se aplica subsidiariamente quando lei especifica o não preveja, ou, seja omissa, ou ainda não o contemple, como é o caso do regime do RGPD, preenchendo a lacuna que se verifica, até á concretização do diploma de execução do RGPD.

Em Portugal esse é um processo que ainda decorre[44], o que poderá, porventura, levar a pensar que o RGPD esteja, assim como que numa espécie de *limbo* até à efetiva concretização da transposição nacional, acima aludida[45].

Assim não é, de facto. O RGPD está em vigor na sua plenitude, somente a sua componente coerciva está suspensa, a aguardar legislação nacional, no entanto mantendo-se em vigor a Lei[46] nacional que impõe coercivamente, o tratamento de dados pessoais, as penalizações ali previstas, impedem um "*vazio*" nesta matéria, e aplicam-se às violações que vierem a ser identificadas[47], participadas e registadas, na autoridade nacional, desde o dia 25 de Maio de 2018.

Quanto ao organismo nacional, é pacífico ser a Comissão Nacional para a Proteção de Dados (CNPD), a exercer a fiscalização que se impõe, uma vez que será convertida em autoridade nacional para a proteção de dados.

1.3.1. Algumas questões peculiares "*Os privilégios do Estado*"

Seja em sede do próprio RGPD, seja em sede da Proposta de Lei do Governo, a questão da isenção de coimas[48] ao Estado tem suscitado legitima celeuma, porquanto subsistir a percepção de que afinal só se exige ao sector privado, o cumprimento do RGPD, ao passo que ao sector público, inexistindo uma sanção sob a forma de coima, este não se sentirá obrigado a fazê-lo.

É certo que a "coima", no quadro das contraordenações, tem uma dupla função, por um lado, penalizar um comportamento ilícito, recorrendo a um meio pecuniário, logo intrusivo na esfera patrimonial do cidadão, por meio do qual se

---

[44] O Governo português apresentou à Assembleia da República a proposta de Lei nº 120/XIII/3ª, tendo a Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias (Processo n.º 6275/2018), remetido à Comissão Nacional de Protecção de Dados (CNPD), para parecer, o que esta fez através do seu Parecer 20/2018, (http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e4554456376524739 6a6457316c626e527663306c7561574e7059585270646d4644623231706333 4e686279396a5a 57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f54493 14d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true), demolidor para a proposta de Lei, queixando-se inclusivamente de não ter sido dada a oportunidade de se pronunciar aquando da elaboração do ante-projecto da Proposta de Lei, o que, segundo afirma, seria de molde a evitar os erros, que adjetivou de "grosseiros", que se deram na proposta do governo.

[45] https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

[46] Lei 67/98, de 6 de Outubro.

[47] Foi já aplicada, pela CNPD, uma sanção de 400.000,00 euros a um hospital por quebra de proteção de dados.

[48] E não "multas" como se vê em alguns escritos sobre a matéria.

opera uma transferência material, pecuniária do particular para o Estado, mas por outro também pedagógico, porque dissuasor, levando o prevaricador a pensar duas vezes, da próxima vez que pensar em repetir a proeza.

No que concerne ao sector privado, é assim. Mas selo-a também no setor público? Quando um ente público paga uma coima, na realidade que tipo de operação temos?

Se um ente público fosse coagido a pagar uma coima, teríamos o Estado a pagar a si próprio, havendo apenas uma espécie de comutação pecuniária entre entes da mesma esfera jurídica – o Estado, razão porque não é difícil aceitar a isenção de coimas aplicadas ao Estado.

Porém, a infração contraordenacional está lá ... Mas as penalizações não têm necessariamente de se revestir de natureza pecuniária, e como se explicará mais à frente, o RGPD assenta num aspeto fulcral que é a RESPONSABILIZAÇÃO. Ora esta não se entende sem um corolário consequente, isto é, mais do que ser coerente, em matéria de responsabilização, é o ser-se consequente, e arcar com as consequências dos atos ilícitos, contraordenacionais, praticados.

Nessa senda, não nos escandaliza que a sanção para o privado sejam as coimas, mas para o público ela terá de forçosamente assentar no estribo da responsabilização pessoal, não pondo de parte nenhuma das várias formas de o fazer, seja com impacto na esfera pessoal do dirigente em causa (responsabilidade financeira)[49], seja com impacto na carreira profissional do mesmo.

Veremos, mas adiante, qual o quadro que impende sobre os eleitos das autarquias, neste particular.

2. Os Direitos de Personalidade e Cidadania, e o RGPD

É nas Constituições que encontramos o suporte de todo o edifício jurídico de um estado, embora não seja condição *sine qua non*, mas é o nosso caso, logo é aí que se encontra, primacialmente, os chamados Direitos de Personalidade, os que diretamente dizem respeito à pessoa jurídica singular.

[49] Obrigatoriedade de retorno, em sede de ressarcimento ao Estado.

A Constituição da República Portuguesa de 1976 (CRP), contém uma imagética antropomórfica interessante49, refletindo, no fundo, que tudo gira à volta do ser humano, da pessoa singular, assim, a CRP contém no seu texto, uma cabeça (titulo I, correspondendo aos direitos e deveres fundamentais), um tronco (titulo II, correspondendo à organização económica), membros (título III, órgãos de soberania) e apêndice (título IV, correspondendo às garantias de revisão constitucional) e o apêndice (corresponde às disposições finais e transitórias).

Por último identifica o cérebro, que tudo comanda, nos artigos iniciais (artº 1º ao 11º, os Princípios Fundamentais), aos quais adjetiva como prólogo.

Veja-se como a tutela constitucional dos direitos de personalidade, começa logo no Artº 1 (antropomorficamente o *cérebro*), o respeitante à dignidade humana, espraiando-se pelos restantes articulados, dos quais se destaca o Artº 13º, o da igualdade, e os Artigos 24º e seguintes respeitantes à vida, integridade física e moral, identidade pessoal, cidadania, etc.

Assim, escorados, os direitos de personalidade, na dogmática constitucional, naquilo que se carateriza por tutela constitucional, ela é como que complementada, ou desenvolvida pela tutela penal[50], a tutela civil [51], e o direito Internacional[52].

A pessoa humana é assim o destinatário primeiro e último do ordenamento jurídico, interno e internacional, razão por que não se compreendia como a devassa da pessoa era, até recentemente, aceite como uma assustadora "normalidade", algo que agora o RGPD, vem colocar um ponto final.

Na verdade, o RGPD insere-se no cerne dos Direitos de Personalidade, pese embora de forma parcelar, uma vez que apenas das pessoas vivas, sendo certo que alguns aspetos das "pessoas"[53] falecidas assistem alguns direitos, como o direito à memória, ao bom nome etc.

Seja como for, a verdade é que o RGPD, vem conferir uma protecção às pessoas singulares, muito acima daquilo que vinha sendo habitual, constituindo-

[50] Onde se tipificam as ofensas mais graves contra a personalidade, como os crimes contra a vida, a integridade física, a liberdade pessoal a honra, a reserva da vida privada, a imagem etc.
[51] Em especial os artº 70 e seguintes.
[52] Convenção Europeia dos Direitos do Homem.
[53] Em rigor e determinando o artigo 66º, nº 1, do código civil português que a personalidade se adquire no momento do nascimento completo e com vida, por maioria de razão extingue-se com a morte, logo o falecido deixa de ser pessoa.

se como um meio, uma ferramenta, para travar a devassa que as novas tecnologias vêm permitindo[54], face à extrema e inusitada facilidade com que terceiros, sem permissão dos visados, escrutinavam as suas vidas, de forma mais ou menos impune.

Esta devassa, e a falta de consequências jurídicas para a mesma, encontram, agora, um regime de proteção vigoroso, e põem em crise práticas ilegais adotadas por uma grande quantidade de empresas e instituições, que se veem compelidas, agora, a cumprir.

Temos pois que a estrita observância do Regulamento Geral de Proteção de Dados, não é uma coisa de somenos, não é apenas mais uma moda legislativa, é isso sim, um regime de salvaguarda para a pessoa singular, é se quisermos, a couraça protetora em que a cidadania plena assenta, qual pilar estruturante da dignidade das pessoas singulares.

Como a cidadania, elemento vital das sociedades, se constrói pela base, é nas comunidades locais, onde se concretizam os princípios da subsidiaridade, política, administrativa, etc, avultando, daí o papel da maior importância que assumem as autarquias locais, nessa construção da cidadania.

3. A Autarquia Local[55], em Portugal, e Cidadania municipal

A Constituição da República Portuguesa, de 1976, instituiu uma matriz de Poder Local escorado em 3 níveis de autarquias, a saber: A Região Administrativa, o Município e a Freguesia, rompendo com a estrutura anterior, da CRP de 1933, assente apenas em Concelhos[56] e Freguesias[57].

Outra novidade introduzida pelo legislador constituinte (1976), foi a criação de novos órgãos: os deliberativos[58], até então inexistentes.

---

[54] O criador, em 1989, do "monstro" *World Wide Web*, **Tim Berners-Lee**, cientista Britânico, da física, numa rara aparição em público, foi a estrela de cartaz na *Web Summit* de Lisboa, este ano, a qual segundo a revista Forbes, "é a maior conferência de tecnologias do mundo", e surgiu a alertar para a necessidade de privacidade na proteção de dados e da privacidade, e que as coisas na *WWW* correram muito mal para o cidadão. Propôs inclusive um contrato social, para a *web*, tripartido – governos, empresas e cidadãos, onde o tópico do respeito da privacidade individual fosse um pilar essencial.

[55] Dias, José António Rajani oliveira, "Cartilha do Eleito Local", edições novaodivelas, 2002, Odivelas.

[56] Embora não se possa considerar os concelhos verdadeiras autarquias, porque não o eram de facto, não passavam de mera administração desconcentrada do Estado.

[57] *Idem*.

[58] Assembleia Municipal e a Assembleia de Freguesia.

E mesmo ao nível dos órgãos executivos, houve alterações importantes: ao nível do município o Presidente da Câmara, deixa de ser simultaneamente administrador do concelho[59], e passa a ser um órgão executivo unipessoal[60], para além de integrar outro órgão, o colegial formado pelo Presidente da câmara[61] e os vereadores[62].

Ao nível da freguesia[63] o formato cingiu-se ao órgão colegial executivo, e à assembleia de freguesia.

A extinção dos cargos de administrador do concelho e do regedor, deveu-se à mudança de paradigma do Poder Local, fundado em autarquias[64], que deixou de ser administração desconcentrada[65] do governo central, para passar a ser administração descentralizada[66] do Estado.

A Região Administrativa[67], sendo um imperativo constitucional (1976), ainda não foi concretizada, pelo que essa não concretização, por parte do legislador ordinário, fá-lo incorrer numa inconstitucionalidade por omissão, desde 1976 até ao presente momento.

Curiosamente, neste particular, temos assistido ao surgimento de movimentos da sociedade civil reivindicando a criação de novos municípios[68] e freguesias, mas nenhum, ainda, reivindicando a instituição das regiões administrativas.

Esta matriz constitucional, acha-se consolidada com novas realidades, desde logo as autarquias, cujo substrato pessoal são os autarcas[69], ou seja todos

---

[59] Antes de 1976 o Presidente da Câmara acumulava as funções de administrador do concelho e nessa qualidade era o representante do Ministro do Interior, na circunscrição concelhia, e supervisionava as polícias nesse território.
[60] À luz do princípio da legalidade, não tendo este órgão unipessoal, competente previsão constitucional, afigura-se de duvidosa constitucionalidade.
[61] Com competências próprias e delegadas pela câmara.
[62] Sem competências próprias mas apenas com competências delegadas e subdelegadas pelo Presidente da câmara.
[63] Antes de 1976 o Presidente de Junta era cumulativamente o Regedor e nessa qualidade representava na circunscrição territorial da freguesia do Ministro do interior.
[64] Termo que provêm da ciência económica de autarcia, isto é, autonomia ou independência administrativa própria.
[65] Cujo instrumento operacional é a **delegação de poderes** no âmbito de uma relação hierárquica subordinada.
[66] Cujo instrumento operacional é a **devolução de poderes**, no âmbito de uma desafetação de atribuições da esfera da administração central para outros entes, independentes e autónomos, sem relação hierárquica.
[67] Dias, José António Rajani oliveira, "O municipalismo em Portugal, Brasil e Cabo Verde", edições OD&F, Funchal, 2006.
[68] Dias, José António Rajani, "O Foral de Odivelas", edições novaodivelas, Odivelas, 2002
[69] Nabais, José Casalta, "A Autonomia Local", edições Almedina, Coimbra, 1990.

os cidadãos recenseados na respetiva circunscrição territorial[70], compostas pelos municípios e freguesias, cujos substratos pessoal são, respetivamente, os munícipes e os fregueses, ou seja – os cidadãos.

A cidadania municipal é pois o exercício livre dos direitos e obrigações, através da participação cívica e cidadã na vida das respetivas autarquias, e neles se concretiza o objeto principal do RGPD, ou seja a defesa dos seus direitos de personalidade.

Assim a responsabilidade, ao nível do poder local, por garantir o cabal cumprimento dos direitos decorrentes do RGPD, para as pessoas singulares, assenta nos ombros dos eleitos locais de forma inexorável, seja ao nível da freguesia, cujos serviços de recenseamento da população, a colocam inevitavelmente a realizar tratamento de dados de toda a população, e do município, cujos serviços à população o colocam a fazer tratamento de dados pessoais em grandes quantidades, basta pensar nas comunidades escolares espalhadas em todo o país e das responsabilidades municipais relativamente a esse universo, para perceber a dimensão de dados pessoais que lhes passa pelas mãos. Estão, pois as autarquias e os seus eleitos, na primeira linha da observância do RGPD.

3.1. O Responsável pelo Tratamento de Dados na autarquia

Nas empresas é fácil perceber quem é o "*responsável pelo tratamento de dados*", é a própria empresa, organização ou instituição, conforme a preferência designativa, e nestas, em regra, a estrutura organizativa tem no seu topo o CEO (gerente, administrador ou diretor geral), que emana as suas ordens através do sistema hierárquico (dirigentes e chefias).

Nas autarquias, já não é assim tão simples. Internamente, um sistema administrativo, de desconcentração, assente numa matriz de delegações de poderes (ou competências)[71], subdelegações de poderes e ou tarefas, e externamente um sistema assente em descentralização de atribuições[72], sujeito

[70] Contrariamente àquilo que se vulgarizou chamar aos eleitos.
[71] Competências são os poderes funcionais que operacionalizam as decisões ou deliberações dos órgãos.
[72] Atribuições são os fins da pessoa coletiva de direito público.

a *Tutela Administrativa*[73], *Poder de Tutela*[74] ou *Regime de Tutela*[75], impõe diferenças e peculiaridades que têm de se levar em linha de conta.

À pouco tempo, num evento promovido em Lisboa[76], foi afirmado que em Portugal vigora a regra da responsabilidade incumbir inteiramente a quem assina um documento, querendo com isto dizer que caberia, por regra, ao decisor máximo da organização, ao CEO, a responsabilidade de tudo, mormente pelo tratamento de dados, seja no público seja no privado.

Não acompanhamos.

No caso das autarquias[77], e tendo presente, por exemplo ao nível do município, que o sistema de administração passa pela existência de um Presidente de Câmara Municipal, com um conjunto muito alargado de competências próprias, umas de caráter interno e administrativas, outras que constituem direitos e obrigações com eficácia externa, fazendo dele um órgão executivo unipessoal, e que a sua ação tanto pode ser direta, como se pode socorrer do instrumento de delegação de poderes, passando responsabilidades e tarefas aos vereadores, bem como aos quadros dirigentes da autarquia, dispersando consideravelmente a sua própria responsabilidade, que fica mitigada.

Os vereadores podem fazer o mesmo com as competências que receberam do presidente, e subdelegá-la ao quadro de dirigentes e colaboradores diretos, incrementando assim a dispersão das responsabilidades.

Mas a Câmara Municipal (o órgão executivo colegial) também tem poderes e competências próprias, que pode delegar no Presidente e este subdelegá-las nos próprios vereadores ou dirigentes.

Já para não falar que muitas deliberações do órgão executivo têm de passar necessariamente pelo órgão deliberativo – a assembleia municipal – que

---

[73] Mera verificação da legalidade dos atos e contratos das autarquias, a que não assiste a apreciação do mérito ou demérito dos mesmos, por violação da autonomia das autarquias.
[74] Consiste no desencadear de auditorias, inspeções ou inquéritos.
[75] Afastamento excecional da autonomia das autarquias consumada na dissolução de órgãos por determinação dos tribunais como consequência de sentença transitada em julgado.
[76] *Privacy Talks* 1ª edição.
[77] A Associação Nacional de Municípios Portugueses, instada pela comissão de assuntos constitucionais da assembleia da república sobre o projeto de proposta de lei nº 120/XIII/3(GOV) pronunciou-se através do parecer de 14 de Maio de 2018, genericamente, aceitando que nos municípios o responsável pelo tratamento dos dados seja a Câmara Municipal, como se prescreve na proposta do governo.

assim se torna num ator importantíssimo neste jogo de responsabilidades partilhadas.

Por tudo isto assume especial importância a responsabilidade solidária, da qual se podem libertar apenas os eleitos que votem vencidos com competente registo do voto vencido e respetiva fundamentação em ata.

Neste quadro não salta à primeira vista quem efetivamente é o responsável pelo tratamento de dados, excetuando uma Lei habilitante[78], em termos concretos, porque em termos abstratos é a pessoa coletiva.

Quanto á responsabilidade recair naquele que apõe a sua assinatura, também é preciso algumas cautelas, pois uma primeira apreciação em diagonal pode induzir em erro, senão vejamos, se um qualquer Presidente de Câmara Municipal assinar, por exemplo, uma licença, no âmbito de um dossier que chegou a si para despacho, devidamente instruído pelos serviços, com a assunção por parte das respetivas chefias da conformidade de todas as regras aplicáveis, e posteriormente se vier a constatar que afinal havia a violação de um Plano Diretor Municipal, é evidente que a responsabilidade não repousa na caneta do presidente, mas sim nas chefias que atestaram erradamente a conformidade do processo.

Outro caso, é o Presidente da Câmara assinar um documento contra o qual até votou contra, registou o seu voto vencido em ata, fundamentado, mas tendo prevalecido uma maioria contra si, deve obrigatoriamente assinar o documento, pois nisso se traduz a consecução da deliberação, e posteriormente vem-se a verificar que a deliberação está ferida de ilegalidade, é também por demais evidente que a responsabilidade não repousa na sua caneta, mas sim no órgão colegial que maioritariamente impôs tal deliberação.

No que concerne ao RGPD e ao responsável pelo tratamento de dados, em alguns municípios, assiste-se à elaboração de Regulamentos Municipais do RGPD, no que se parece conformar-se redundantemente com o Regulamento Europeu, estabelecendo, aqueles, por exemplo, que o Presidente da Câmara é o Responsável do Tratamento dos Dados[79], com base na circunstância daquele representar o município em juízo. Oferece-nos algumas dúvidas da pertinência

[78] *Idem*.
[79] A ANMP no seu parecer esclarece preferir a redação da proposta do governo que impõe essa condição à Câmara Municipal ao invés do seu presidente.

de semelhantes regulamentos municipais, exceto se na base estiver a implementação de um Sistemas de Gestão Municipal de Proteção de Dados, o que se afigura aceitável, mesmo considerando que a prazo o IPAC irá acreditar instituições emitentes de certificação ao abrigo de uma norma nacional para esse efeito.

Em conclusão, é preciso muita atenção na análise das responsabilidades, antes de se apontar o dedo a quem assina. É preciso estar muito familiarizado com o setor público em geral e o autárquico, em particular, para se darem passos seguros na identificação das responsabilidades, no âmbito do tratamento de dados, numa autarquia.

3.2. O Oficial da Protecção de Dados – Data Protetion Officer (DPO) na autarquia

O RGPD cria uma figura que configura uma nova profissão no domínio da proteção de dados – o Responsável da Proteção de Dados, tradução portuguesa do "*Data Protetion Officer*".

A obrigatoriedade, para o sector público é uma das regras, pelo que nas autarquias, sejam elas os municípios sejam elas as freguesias, forçosamente, na maioria delas, terá de existir um profissional para exercer esta função[80], pese embora a senhora presidente da CNPD, tenha afirmado na RTP3, coisa diferente[81]. O problema coloca-se ao nível das freguesias[82] com diminuto tratamento de dados, algo que já no parecer da ANMP, sobre esta matéria, é referido como sendo necessário esclarecer o alcance de "*em função do volume de dados tratados*" da Proposta de Lei de execução do RGPD ... no entanto, por analogia, será de seguir a regra, já estabelecida no RGPD para as empresas que tenham mais de 250 colaboradores serem obrigadas a terem um DPO, caso disposição diversa não seja definida.

[80] http://www.radiocruzeiro.pt/opiniao-cruzeiro-a-protecao-de-dados-nas-autarquias-locais/
[81] https://www.rtp.pt/play/p4259/e358376/fronteiras-xxi (ao minuto 52 do programa.)
[82] Todos os municípios têm tratamento de dados acima desse montante.

O sistema de capacitações de um profissional destes inclui, necessariamente: Perfil[83], Caracterização[84], Missão[85], Estatuto[86], Incompatibilidades[87].

O primeiro passo para demonstrar que a atuação da autarquia está em linha com o espírito do regulamento são coisas tão básicas como:

a) a nomeação de um DPO, publicá-lo em competente edital[88], e, cumulativamente, na revista municipal ou boletim informativo, consoante o caso, e no site da autarquia, bem assim como publicitação dos seus contactos (diferenciados dos restantes da autarquia);

b) envolver todos os colaboradores da autarquia em ações de carácter formativo[89] e de sensibilização[90].

Sem isto, o cidadão (munícipe ou freguês) fica objetivamente impedido de se dirigir ao único profissional em quem o RGPD atribui poderes, exclusivos, no âmbito da proteção de dados, constituindo, naquilo que se caracteriza como uma denegação de justiça por parte dos eleitos, e se reiterada evolui para uma caracterização de abuso de poder, substancialmente mais grave.

É certo que haverá quem repouse a sua consciência na previsível isenção de coimas por incumprimento do RGPD, porém, será de atentar com cautela, que as sanções específicas do RGPD não são as únicas a serem assacadas aos eleitos locais, porquanto estes têm outros normativos que sancionam condutas ilícitas ou ilegítimas[91], como será o caso.

É, pois, preocupante que à data de 21 de Agosto de 2018, "apenas" 11 municípios e 3 freguesias tenham comunicado a nomeação dos respetivos DPO à Comissão Nacional de Proteção de Dados. Mesmo que entretanto tenha

[83] https://lisboatv.pt/2018/10/03/rgpd-dpo-perfil/
[84] https://lisboatv.pt/2018/10/01/rgpd-dpo-caracterizacao/
[85] https://lisboatv.pt/2018/10/05/rgpd-dpo-missao-funcoes/
[86] https://lisboatv.pt/2018/10/06/rgpd-dpo-estatuto/
[87] https://lisboatv.pt/2018/10/02/rgpd-dpo-incompatibilidades/
[88] A nomeação deve fazer referência, caso se trate de um recurso humano interno, que outras funções ele exerce.
[89] Decisivo, em especial para quem trate dados pessoais na autarquia.
[90] Muito importante para os restantes colaboradores que não se incluam na nota anterior.
[91] Lei da Tutela Administrativa nº 27/96de 1 de Agosto de 1996, determina a perda de mandato ou dissolução de órgãos, no caso de se "incorrer por acção ou omissão dolosas, em ilegalidade grave traduzida na consecução de fins alheios ao interesse público (alínea d) do nº 1 do Artigo 8º, conjugado com alínea i) do artigo 9º).

havido algum incremento naqueles números, ficarão certamente bem longe do que seria desejável num universo de milhares de autarquias portuguesas, sobretudo porque a maior parte delas[92] é responsável pelo recenseamento da população, tendo por isso a responsabilidade do tratamento de milhões de dados pessoais.

Aqui chegados, impõe-se a questão: quem, nas autarquias tem a competência para nomear o DPO, sendo certo que a proposta de Lei aponta para os respetivos presidentes?

É simples, de acordo com o RGPD compete ao responsável pelo tratamento dos dados a nomeação do DPO, ora nas autarquias em abstrato isso é atribuído à pessoa coletiva, mas em concreto compete, no município ao seu Presidente de Câmara, não porque seja ele que representa em juízo o município mas porque lhe são conferidas essas competências[93], já na freguesia compete[94] ao órgãos colegial (Junta de Freguesia), pelas mesmas razões aduzidas para o município, restará depois, casuisticamente, perceber se há ou não delegações e/ou sub-delegações de competências, nessa matéria.

4. Conclusões

São Bernardo de Claraval, Doutor da igreja católica, mentor de 2 Papas, Santo da igreja, e ideólogo do nascimento de Portugal[95], tinha por lema "***Enganei-me? pois não importa, estou sempre disponível para me corrigir***", isto para significar que o erro, seja por negligência, seja por intenção, desde que corrigido pode até ser uma oportunidade de melhoria.

O RGPD entrou em vigor em 25 de Maio de 2018, foi um erro o Poder Local não se ter preparado para o seu impacto, como o demonstra a exiguidade de autarquias que o acolheram, mas parafraseando a sabedoria popular, "*mais vale tarde que nunca*" , desde que se demonstre uma real vontade para ir ao encontro do Regulamento, seja promovendo a necessária nomeação de um Responsável de Proteção de Dados (DPO), seja envolvendo os respetivos recursos humanos nas tão necessárias ações de sensibilização e formação, para

[92] As freguesias.
[93] Alínea a), c) e d) do nº 2, do artigo 35º, da Lei 75/2013, de 12 de Setembro.
[94] Alínea b), e e) do artigo 19º do mesmo diploma legal.
[95] Dias, José António Rajani Oliveira, "Portugraal O Reino Templário", ensaio histórico, edições Verbos e letras, 2011.

que os cidadãos estejam minimamente descansados quanto ao tratamento dos seus dados pessoais, e terá valido a pena.

Este é um processo lento, moroso, mas necessário porque implica uma mudança de paradigma – de um total laxismo no que concerne à privacidade, à proteção dos direitos dos cidadãos vai um longo caminho – escorado numa mudança de mentalidades, algo socialmente complexo e pejado de resistências que é preciso ir vencendo.

As autarquias e os seus eleitos locais têm aqui um papel crucial, e central, indelegável, porque lhe compete a prossecução dos interesses dos seus cidadãos, numa quase metamorfose das suas novas responsabilidades, sempre em crescendo desde o longínquo ano de 1977[96], data em que o poder local se concretizou de facto.

Bibliografia

Dias, José António Rajani Oliveira**, "***A Cartilha do Eleito Local***",** edições NovaOdivelas, Odivelas, 2002.

Dias, José António Rajani Oliveira**, "***O Foral de Odivelas***",** edições NovaOdivelas, Odivelas, 2002.

Dias, José António Rajani Oliveira**, "***O Municipalismo em Portugal, Brasil e Cabo Verde***",** edições OD&F, Funchal, 2006.

Dias, José António Rajani Oliveira**, "***Portugraal o reino templário***",** Ensaio**,** edições Verbos e Letras, Lisboa, 2011.

Dias, José António Rajani Oliveira**, "***O Poder Local nas Constituições Portuguesas***",** Ensaio**,** edições Artelogy, Vila Nova de Gaia, 2016.

Nabais, José Casalta, "A Autonomia Local", edições Almedina, Coimbra, 1990.

[96] Ano em que saiu a primeira legislação sobre autarquias locais, depois de aprovada a Constituição da república Portuguesa de 1976.

O RGPD e o impacto nas organizações: 6 meses depois - o caso particular das instituições do ensino superior

Daniel Francisco[1]

Resumo

Numa altura onde ainda existem muitas dúvidas sobre as particularidades das instituições de ensino superior e algumas polémicas que surgem na comunicação social sobre a aplicação do Regulamento Geral de Proteção de Dados (RGPD), pretende-se conhecer algumas especificidades normativas das instituições de ensino superior (legislação e deliberações).

O RGPD é um desafio incontornável para as organizações, implicando a adoção de um conjunto vasto de medidas técnicas e organizativas não planeadas.

Quais são algumas das realidades especificas das instituições do ensino superior?

Como conhecer e identificar o enquadramento legal da proteção de dados pessoais resultantes do (RGPD) em articulação com as funções desenvolvidas numa instituição de ensino superior?

Como conseguir identificar os principais conceitos e os princípios enquadradores do RGP?

Como compreender a transversalidade da temática da proteção de dados no universo da Instituição de ensinos superior (alunos, funcionários, docentes e demais colaboradores?

Como compatibilizar os comportamentos dos colaboradores com o paradigma do RGPD?

Como tratar o caso de transferência de dados de alunos, funcionários e docentes em mobilidade para países terceiros e os seus dados?

[1] Daniel Fernandes do Carmo Francisco. Doutorado em Comunicação Empresarial e Institucional na Universidade Complutense de Madrid, Investigador, Formador e Consultor de implementação na área de RGPD. Docente no ensino superior. Autor e Conferencista.

O novo Regulamento Geral de Proteção de Dados (RGPD) é um desafio.

Sobretudo para organizações tão vivas e dinâmicas comos as instituições de ensino superior. Estas organizações quer pelo seu core Business, quer pela sua organização e serviços académicos quer ainda pela ligação e redes de contactos nacionais e internacionais, movimentam em grande escala uma multiplicidade de dados.

E algumas vezes ficam tao espartilhados que acontecem noticias como esta:

UNIVERSIDADE DE LISBOA ANUNCIA O FIM DAS AFIXAÇÕES PÚBLICAS DE NOTAS[2]

Ou esta

REGULAMENTO DE PROTEÇÃO DE DADOS PODE ORIGINAR PERDA DE INFORMAÇÃO[3]

A Secretária de Estado do Ensino Superior alertou que é preciso "respeitar, em quaisquer circunstâncias, a privacidade e defesa dos direitos", mas com "equilíbrio e bom senso"

Como sobreviver a estes desafios mantendo o bom-senso, sem perder informação e sem deixar de cumprir as suas obrigações e fornecer um serviço de excelência?

As instituições devem conhecer o novo quadro legal e estar preparadas para cumprir as novas regras e obrigações atuais e futuras sobre a temática da proteção de dados.

Não só para evitar coimas e sanções, mas também para evitar entropias e efeitos de imagem e reputação negativos junto dos seus públicos-alvo.

Assim, iremos abordar 6 tópicos:

- 1 – Princípios de Licitude e de Legitimidade
- 2 – Controlo de acessos
- 3 – Transferências para países terceiros
- 4 – Gestão de consentimentos
- 5 - Projeto de Diretriz n.º 1/2018

[2] https://www.sabado.pt/portugal/detalhe/universidade-de-lisboa-anuncia-o-fim-das-afixacoes-publicas-de-notas

[3] https://www.dn.pt/portugal/interior/secretaria-de-estado-do-ensino-superior-alerta-para-risco-de- perda-de-informacao-com-regulamento-de-protecao-de-dados-9263360.html

• 6 - Deliberação n.º 1495/2016

Iremos neste artigo focar-nos sobretudo no universo das instituições de Ensino Superior Públicas, devido as suas características particulares, mas muito do que iremos abordar aplica-se igualmente às Instituições de ensino superior privadas.

Desenvolvimento

1 - Princípios de Licitude e de Legitimidade

As organizações de Ensino superior não se podem esquecer dos artigos 5º e 6º do RGPD. Estes são os artigos do RGPD que abordam a questão da Licitude e da Legitimidade. Como indicado pela Comissão Europeia:

"As administrações públicas estão sujeitas às regras do RGPD sempre que efetuam o tratamento de dados pessoais relacionados com um indivíduo. Cabe às administrações públicas nacionais a responsabilidade de prestar apoio às administrações regionais e locais na preparação para a aplicação do RGPD.

A maior parte dos dados pessoais detidos pela Administração Pública são habitualmente tratados com base numa obrigação jurídica ou na medida do necessário para realizar tarefas por motivos de interesse público ou no exercício de autoridade pública de que está investida."[4]

Esta frase assenta numa das especificidades das instituições de ensino superior públicas, o serem públicas, realizarem tarefas por motivos de interesse público e estarem investidas de exercício de autoridade pública.

Estas especificidades são essenciais e deveras importantes na maneira como temos de focalizar a abordagem dos restantes tópicos. As instituições de Ensino Superior avançam por norma, na prática, com 3 pilares de legitimidade para tratar dados pessoais.

Conforme diz o artigo 6º do RGPD: "1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

[4] Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_pt

b)O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica."

No entanto as organizações públicas não estão isentas de cumprir o artigo 5º do RGPD:

"1. Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»);

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);

2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»).”

Assim mesmo que as organizações públicas no futuro, como esteve previsto no projeto da Proposta de Lei 120/XIII[5], não sejam abrangidas pelas aplicação de coimas da CNPD, não deixarão de estar sujeitas a controlos que estejam sob as alçadas dos sistemas de controle interno (Inspeções setoriais, Tribunal de Contas etc.) nem de todas as demais responsabilidades existentes no panorama legislativo nacional, além de possíveis infrações que possam ser cometidas.~

2 – Gestão de dados e Controlo de acessos

Este será sem dúvida um dos piores e maiores dilemas e desafios para uma organização:

Primeiro: Como conseguir identificar e mapear os dados que possui, e

Segundo: Como verificar que se encontram em conformidade com o RGPD.

[5] Proposta legislativa que visava assegurar a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

Terceiro: Como garantir que esses dados estão em segurança e não apresentam um risco para o titular dos dados.

O RGPD permite o uso dos dados necessários para funcionamento da organização, mas têm de estar claramente definida a necessidade de processar os dados pessoais.

Por exemplo quando os alunos se registrarem, as instituições vão querer ser transparentes e cumprir integramente o direito de informação ao titular dos dados, até porque quantos mais dados pessoais se recolhe, quanta mais informação se tem de dar.

Especificamente, deverão saber por que precisam desses dados, por quanto tempo os vão manter e onde está armazenada essa informação, para a poder proteger e armazenar em segurança.

Outra área a que se deverá estar atento, é quando se contrata pessoal, nessas situações é necessário fornecer informações sobre como os dados pessoais são processados e a quem são transmitidos e aqui uma vez mais, como a relação está dependente do cumprimento contratual (Artigo 6º do RGPD) há legitimidade para o tratamento, mas também existe obrigação de informação (Artigo 12º e 13º do RGPD).

Assim, face a todos esses dados que existem na organização, a mesma deve de estar atenta à sua segurança e a quem os acede. E nunca esquecendo conforme diz o artigo 2º do RGPD: "1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados."

Os dados pessoais guardados em suportes físicos não informatizados, isto é por exemplo em papel, estão sujeitos às mesmas regras.

Uma das regras de proteção dos dados contra acessos desnecessários, envolve que apenas deve aceder quem precisa para efeitos do tratamento e isso implica que o modelo hierárquico não chega e que deve haver registo dos acessos a dados pessoais.

Não esquecer o que é que constitui uma violação da privacidade e dos dados pessoais. Segundo o artigo 4º/12: "«Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados

pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

Assim um acesso não autorizado ou acidental, a dados pessoais recolhidos e tratados por uma instituição de ensino superior, é uma violação de dados pessoais.

Acessos de pessoas dentro da organização (alunos, professores, funcionários e demais colaboradores internos ou externos) indevidos a informações pessoais, coloca a organização em incumprimento do RGPD.

E para nos alertar, a coima instituída pela CNPD ao Hospital do Barreiro de 400 mil euros,[6] deve- se sobretudo na argumentação apresentada, e face a uma deficiente política de controlo de atribuições e controlos de acessos, que permitiam consultar dados e informações pessoais e clínicas (dados especiais abrangidos pelo artigo 9º do RGPD, onde se inserem os dados sobre saúde).

O RGPD introduz em todas as organizações o dever de reportar certos tipos de violação de dados à entidade supervisora de cada país (art.º 33º) e aos indivíduos afetados (art.º 34º) consoante determinadas condições. Uma violação de dados, como visto, consiste numa falha de segurança, que pode levar à destruição, perda, alteração, divulgação não autorizada, ou acesso a dados pessoais. Isto significa que uma violação de dados pessoais, é mais do que perder apenas dados pessoais.

Apesar de a CNPD ter de ser notificada de uma violação de dados pessoais, se essa falha apresentar riscos elevados, para os direitos e liberdades dos indivíduos (art.º 33º /1), nomeadamente, provocar efeitos de detrimento como descriminação, ameaça à reputação, perda financeira, perda de confidencialidade ou qualquer outra desvantagem social ou económica significativa, ainda assim internamente a organização tem de tomar medidas técnicas e organizativas, que minimizem ou atenuem o risco para o titular dos dados.

Este processo de violação tem de ser tratado caso a caso, tem de ficar registado na organização e pode originar danos reputacionais elevados.

[6] http://exameinformatica.sapo.pt/noticias/mercados/2018-10-19-CNPD-Hospital-do-Barreiro-multado- em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos

3 – Transferências para países terceiros

As Instituições de Ensino Superior, num mundo globalizado e competitivo têm cada vez mais de abrir os seus horizontes, promovendo-se em espaços geográficos cada vez mais amplos para captar alunos, professores, investigadores e obter parcerias estratégicas vitais para o seu desenvolvimento.

Isto levanta a questão de intercâmbios de recursos humanos tais como o projeto ERASMUS e outros de mobilidade de pessoas (e leia-se também de titulares de dados) para dentro e para fora das próprias instituições.

Nessa mobilidade e nos seus processos de candidatura existe troca de informação e de dados pessoais, para os que enviamos e para os que recebemos, e muitas vezes esses dados são transferidos para fora do espaço geográfico da U.E.

A questão de transferência de dados para países fora da U.E. é bastante importante. Com uma agravante, a maioria das orientações fornecidas pela Comissão Europeia encontram-se em inglês, sendo que só alguns poucos documentos estejam traduzidos para português. (O documento essencial sobre os modelos de clausulas tipo é reproduzido nos anexos).

Realçamos que a Comissão Europeia tem o poder de determinar, com base no artigo 45º do RGPD se um país fora da UE oferece, ou não, um nível adequado de proteção de dados, quer seja pela legislação interna desse país quer seja pela assunção e reiteração de compromissos e acordos internacionais que tenha assinado.

O número 1 do Artigo 45º do RGPD tem na sua redação o seguinte: “1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.”

Assim como diz o Regulamento para os países para os quais haja acordo, não é necessário ou exigida autorização especifica para a transferência de dados pessoais.

O que levanta a questão pertinente de que transferências de dados pessoais para os outros países terceiros sobre os quais a Comissão Europeia não tenha ainda decidido como fiáveis requererem cuidados e medidas

adicionais e especiais, mesmo que se tenha o consentimento do titular dos dados.

Conforme diz a Comissão europeia “As regras da UE em matéria de proteção de dados aplicam- se ao espaço económico europeu (EEE), que inclui todos os países da UE e países terceiros Islândia, Liechtenstein e Noruega.

Quando os dados pessoais são transferidos para fora do espaço económico europeu, são previstas salvaguardas especiais para garantir que a proteção viaja com os dados.

A reforma da legislação comunitária em matéria de proteção de dados adotada em 2016 oferece um conjunto diversificado de mecanismos de transferência de dados para países terceiros: decisões de adequação, regras contratuais-tipo, regras vinculativas, mecanismos de certificação, códigos de conduta, as chamadas "derrogações " etc.

Embora a arquitetura do regime das transferências internacionais seja semelhante à da Diretiva relativa à Proteção de Dados de 1995, a reforma simplifica e expande a utilização dos mecanismos existentes e introduz novas ferramentas para as transferências internacionais.

Após ter completado a reforma da legislação comunitária em matéria de Proteção de Dados, a Comissão adotou uma estratégia de promoção das normas internacionais de privacidade. A sua comunicação de 10 de janeiro de 2017 apresenta a sua abordagem no desenvolvimento de decisões de adequação, bem como outras ferramentas para transferências e instrumentos internacionais de Proteção de Dados.”[7]

Assim a quem tenha de tratar ou decidir sobre estas questões é essencial ler a “COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO - Intercâmbio e proteção de dados pessoais num mundo globalizado”[8] para verificar qual será o mecanismo e as ferramentas mais útil e funcionais a utilizar para a transferência de dados que tem de efetuar.

E conhecer a lista de países e territórios considerados legítimos pela U.E.

---

[7] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/rules-international-transfers-personal-data_pt

[8] Disponível em português em:

https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

Como proceder então no caso de transferência de dados pessoais para países e territórios ainda não reconhecidos como seguros ou compatíveis com U.E.?

A Comissão Europeia tem indicado que as cláusulas contratuais-tipo oferecem salvaguardas suficientes para a proteção de dados dos dados a transferir internacionalmente.

Até à data, a comissão, emitiu dois conjuntos de cláusulas contratuais-tipo para as transferências de dados de Responsáveis de dados na UE para os Responsáveis de dados estabelecidos fora da UE ou do espaço económico europeu (EEE), que as instituições de ensino superior deverão incluir nos seus protocolos com instituições de ensino superior.

Também emitiu um conjunto de cláusulas contratuais para transferências de dados de Responsáveis na UE para subcontratantes estabelecidos fora da UE ou do EEE.

4 – Gestão de Consentimentos

Este tópico para as instituições de ensino superior é curto, conforme verificamos no primeiro tópico a necessidade de pedido de consentimento nas instituições de ensino superior publico é residual.

No entanto é essencial as organizações saberem muito bem para que dados pessoais e tratamentos efetuados, se requer consentimento.

Assim onde aplicável, o consentimento para processamento e tratamento de dados pessoais precisa ser solicitado, obtido e armazenado como prova.

Por exemplo para alunos com idade menor de consentimento precisarão dos pais para assinarem o consentimento. Não nos podemos esquecer que cada vez entram mais alunos menores de idade para o ensino superior, mesmo que seja por meros meses.

5 - Projeto de Diretriz n.º 1/2018

É interessante observar que o primeiro processo de consulta pública efetuado pela CNPD para uma diretriz foi sobre "**Disponibilização de dados pessoais dos estudantes e dos docentes no sítio da Internet das instituições de ensino superior".**

Esta diretriz esteve em consulta publica até 4/09/2018, e aborda a "Disponibilização de dados pessoais dos estudantes e dos docentes no sítio da Internet das instituições de ensino superior".

Isto revela a importância que as instituições de ensino no seu todo, devem ter no seu funcionamento sobre as questões sobre dados pessoais.

1.Disponibilização de dados pessoais dos estudantes

1.1. Pautas de classificação

"…das pautas apenas devem constar os dados pessoais estritamente necessários ao cumprimento da finalidade de publicitação da avaliação dos estudantes, ou seja, somente o nome e número de cada aluno com a correspondente avaliação quantitativa por disciplina (para além do ano de inscrição e porventura a turma).

Para atingir a finalidade da publicitação das classificações, não há qualquer necessidade de introduzir nessa pauta informações adicionais, tais como as faltas do aluno, a existência de eventual apoio social escolar ou outra informação que, existindo na ficha individual do aluno ou noutros registos, será sempre excessiva em relação ao objetivo que a pauta visa cumprir."

De todo o modo, e por aplicação ainda do princípio da proporcionalidade, a publicação de pautas na Internet não deve ser feita em página aberta e acessível a qualquer um, não apenas por alargar substancialmente o leque de destinatários, extravasando o fim pretendido, como também pelo impacto que a sua disponibilização na Internet tem na esfera jurídica dos estudantes.

Por isso a CNPD estabeleceu como orientação para os estabelecimentos de ensino a não publicação de pautas de avaliação de alunos em sítios da Internet de acesso livre.

As pautas entretanto publicadas na Internet devem, pelas razões expostas e por força da alínea c) do n.º 1 do artigo 5.º do RGPD, ser retiradas da Internet, tendo o cuidado de forçar o apagamento dos dados em cache nos motores de busca.

Como fica então a função publica de transparência e informação das Pautas?

O projeto diz:

"Todavia, compreende-se também que, deste modo, não fica satisfeito o dever de publicitação, acima referido, razão por que deve, nestes casos, assegurar-se a

afixação das pautas nos locais próprios no interior do estabelecimento de ensino, por um período de tempo razoável.

De todo o modo, tem de ser garantido o acesso à pauta ao restantes estudante objeto de avaliação, enquanto interessados nesta informação, para precisamente poderem aferir do respeito pelos princípios da igualdade e da justiça no procedimento de avaliação (v.g., por consulta da pauta na secretaria ou pedido de certidão)."

1.2. Decisões de natureza disciplinar e outro tipo de informações pessoais

Deve também garantir-se que decisões tomadas no âmbito de processos disciplinares não sejam tornadas públicas ou dadas a conhecer a quaisquer terceiros dentro da comunidade académica.

Recorde-se que a publicação de atos administrativos só é obrigatória quanto imposta por lei (cf. 159.º do Código do Procedimento Administrativo), sendo certo que a Lei n.º 62/2007, de 10 de setembro, que define o regime jurídico das instituições de ensino superior, não prevê a publicidade de decisões de aplicação de sanções disciplinares aos estudantes.

Analisados aqueles diplomas legais, conclui-se pelo afastamento legal da publicitação das decisões sancionatórias, como bem espelha o artigo 58.º da Lei n.º 58/2008, de 9 de setembro. Mas ainda que a lei não o dissesse expressamente, ao mesmo resultado se chegaria pela ponderação dos direitos e interesses em presença e a sua harmonização à luz do princípio da proporcionalidade."

2- Dados pessoais dos docentes e demais trabalhadores da instituição de ensino superior

2.1. Relatórios sobre inquéritos pedagógicos

"Finalmente, esclarece-se que a publicação de relatórios com avaliação dos docentes não tem o mesmo enquadramento jurídico que a avaliação dos estudantes. Isto porque a afixação das pautas de classificação dos alunos tem na sua base um princípio de publicidade legalmente imposto e concretizado em regulamentos administrativos, que visam garantir a transparência e o controlo da atividade do ensino e a igualdade entre os estudantes.

Ou seja, assegurando-se que a informação é disponibilizada on-line, em acesso restrito, à comunidade docente, com informação agregada da avaliação do

conjunto das disciplinas por ano curricular, ou do conjunto das disciplinas no curso, dando-se a conhecer a cada um dos docentes apenas a respetiva avaliação.

Sem prejuízo, obviamente, de o resultado da avaliação, com a informação completa e, portanto, integrando dados pessoais, dever ser do conhecimento de todos os que dentro da comunidade académica estão legitimamente em condições de tomar decisões a partir da análise da informação dele constante (v.g., diretor, responsável pela disciplina e avaliadores em sede do procedimento de avaliação de desempenho)."

2.2. Avaliação de desempenho

"…..Assim, não se apresentando como imprescindível esta disponibilização on-line para garantir o conhecimento da informação pelos interessados diretos, e não sendo a disponibilização por esta via facilmente concretizável sem expor a informação aos docentes que não integram o universo desses interessados diretos, a CNPD conclui não ser admissível a disponibilização dos resultados da avaliação de desempenho no sítio da Internet das instituições de ensino superior."

"2.3. Decisões de natureza disciplinar

Com os fundamentos expostos supra, em 1.2., também as decisões sancionatórias que tenham como destinatários docentes ou demais trabalhadores das instituições de ensino superior não devem ser tornadas públicas ou dadas a conhecer à comunidade académica.

Com efeito, nem a função punitiva, nem a função pedagógica ou preventiva da sanção disciplinar parecem exigir mais do que a aplicação da sanção e a sua notificação ao destinatário respetivo, sendo certo que a divulgação generalizada por terceiros de tal sanção implicaria uma restrição desnecessária e excessiva do direito à proteção de dados pessoais sujeitos a um especial regime de proteção, previsto no artigo 10.º do RGPD, em violação do princípio da proporcionalidade previsto na alínea c) do n.º 1 do artigo 5.º do RGPD."

6 - Deliberação n.º1495/2016

Existe no projeto de **Diretriz n.º 1/2018** uma nota de rodapé na página, a quarta, que diz o seguinte:

Esta orientação vem vertida na Deliberação da CNPD n.º 1495/2016, de 6 de setembro. Embora a referida deliberação seja diretamente dirigida aos

estabelecimentos de educação e de ensino não superior, o teor das conclusões do ponto 1.1., págs. 7-9, é aplicável, com as devidas adaptações, aos estabelecimentos de ensino superior[9].

Esta nota é importante, porque até como a nota diz, há matéria na Deliberação n.º 1495/2016 que a CNPD considera que com as devidas adaptações, é aplicável às instituições de ensino superior.

Na Deliberação n.º 1495/2016, de 6 de setembro, a CNPD definiu orientações precisas às Escolas sobre os limites legais para o tratamento de dados pessoais, na vertente da sua difusão através da Internet, bem como sobre os procedimentos que devem adotar com vista a aumentar a segurança da informação e a minimizar os riscos de utilização abusiva dos dados pessoais.

E nas páginas 7 a 9 é abordado o tema: 1. O dever de publicidade e a sua concretização.

A deliberação diz que "A utilização generalizada da Internet pelos estabelecimentos de ensino, com destaque para a criação de sítios (websites) próprios veio contribuir inevitavelmente para uma aproximação da escola à sociedade, através de uma maior exposição das suas atividades, bem como permitindo o contacto direto, célere, económico e eficiente de alunos, encarregados de educação e pessoal docente e não docente.

No entanto, a rápida adesão a estes meios tecnológicos não foi, em geral, acompanhada pelo estabelecimento de critérios rigorosos que enquadrassem a disponibilização de informação pessoal na Internet, de modo a acautelar a defesa dos direitos das crianças, designadamente o direito à proteção de dados pessoais e à privacidade"[10].

Conclusões

Assim, embora aparentemente nestes seis meses, pareça não ter acontecido nada de especial, no que diz respeito às particulares situações das Instituições de ensino superior, podemos ver que já algo se passou.

[9] Disponível em https://www.cnpd.pt/bin/consultapublica/Projeto_de_Diretriz_1_2018_disponibilizacao_dados_on- line_instituicoes_ensino_superior.pdf

[10] Disponível em https://www.cnpd.pt/bin/orientacoes/DEL_1495_2016_dados_alunos_Internet.pdf

Tais mudanças advieram de algumas orientações da CNPD, autoridade nacional de controlo e da sua linha de pensamento interpretativa do RGPD, o que desde já permite às instituições de ensino superior começarem a avaliar a sua conformidade.

Assim focalizando sempre a melhoria continua, a avaliação e o controlo que devemos começar a realizar das medidas que se implementaram, torna vital fazer uma análise de conformidade com a linha de pensamento e orientações da CNPD, adaptando-as à realidade da instituição.

No fim torna-se essencial mais um aspeto: o continuar a sensibilizar todos os colaboradores para a importância da temática da proteção de dados.

O RGPD está vivo, de boa saúde e em evolução, não convém adormecer nem abrandar o ritmo.

Referência das Fontes

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and- organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data- protection-regulation-gdpr-public-administration-should-be-aware_pt

https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/rules-international- transfers-personal-data_pt

https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

https://www.cnpd.pt/bin/consultapublica/Projeto_de_Diretriz_1_2018_disponibilizacao_dados_on- line_instituicoes_ensino_superior.pdf

https://www.cnpd.pt/bin/orientacoes/DEL_1495_2016_dados_alunos_Internet.pdf

Dezembro de 2018

A proteção de dados no sistema tributário português

Rui Miguel Zeferino Ferreira[1]

Introdução

Na presente época de pós-modernidade os cidadãos e os governos são confrontados com novos desafios de governança, impostos pela sociedade e pela economia digital, a que o mundo do direito não pode deixar de tentar encontrar os necessários *checks-and-balances* no debate dialético entre a necessidade de desenvolvimento da construção digital da sociedade e de proteção da informação e dos dados pessoais dos cidadãos. Efetivamente, o dilema centra-se na necessidade de não impor entraves ao desenvolvimento tecnológico, mas ao mesmo tempo garantir uma adequada segurança e confidencialidade, resultantes da utilização de tecnologias de controlo, vigilância e segurança na transmissão de dados informatizados, que permitem, por um lado, processar, armazenar e transmitir grandes quantidades de informação e, por outro, permitem à escala global a transferência de informação e a localização em tempo real.

Esta realidade levanta o problema da transferência para terceiros de informação sensível, em muitos casos com efetivo desconhecimento dos afetados. Em causa estão informações e dados pessoais relativos ao nome, género, filiação, morada, profissão, dados relativos à sua saúde, incluindo os genéticos, dados relativos à sua situação financeira, patrimonial e fiscal, às suas opções de consumo e aos seus posicionamentos políticos e religiosos, que podendo ter um fim específico, licito e até conhecido à priori, encerram riscos de utilizações indesejadas, indiscriminadas e fraudulentas por parte de terceiros, ao permitirem a criação de perfis, utilizáveis para os mais variados efeitos, e que

[1] Professor-Adjunto no Instituto Superior de Entre Douro e Vouga (ISVOUGA). Professor-Assistente Convidado no Instituto Politécnico de Bragança (IPB). Investigador da Universidade de Santiago de Compostela (USC), Espanha. Juiz-Árbitro no Centro de Arbitragem Administrativa (CAAD). Advogado.

no limite podem conduzir a fenómenos de roubo de identidade[2] ou apagamento de cidadãos da sociedade[3].

Por seu lado, na presente pós-modernidade é fatal a existência de renúncia a alguns direitos fundamentais, outrora sacralizados pelo direito, como sucede com a reserva da intimidade da vida privada, em particular como consequência de exigências jurídico-administrativas ou jurídico-tributárias, exercidas por órgãos públicos, sob o *ius imperium* que lhes está conferido. No campo do sistema tributário surge uma tensão entre a liberdade dos cidadãos, sem ingerência do Estado nas opções e comportamentos que adota, com a obrigação de dar cumprimento a deveres jurídicos impostos pela lei, que implicam a recolha, tratamento, armazenamento e utilização dos dados pessoais dos cidadãos, nomeadamente, com fundamento na luta contra a fraude fiscal, entendida como um fim em si mesma. Ora, este tratamento efetuado pelo Estado vem levantando vários problemas de segurança, derivado às fragilidades técnicas dos sistemas do Estado, bem como ao nível da confidencialidade dos modelos organizativos existentes, que facilitam a usurpação e o acesso ilegítimo de terceiros aos dados utilizados licitamente pelos órgãos da administração tributária[4].

Na realidade o dever de colaboração e de comunicação de dados com relevância tributária constitui nesta arquitetura um instrumento fulcral, quer para garantir a justa tributação, quer para garantir a eficácia da gestão tributária. Esses dados pessoais são tidos como essenciais a uma atuação eficaz da administração tributária, pelo que a sua utilização é justificável mesmo quando seja incomoda para o cidadão. Pois, sustenta-se que sem uma adequada informação não poderia existir a comprovação do cumprimento das obrigações tributárias, nem se daria o efeito psicológico de induzir os contribuintes a

---

[2] Neste sentido, TEIXEIRA, Guilherme da Fonseca, "Identidade e autodeterminação informacional no novo Regulamento Geral de Proteção de Dados: a inevitável privatização dos deveres estaduais de proteção", in *Católica Law Review*, volume II, n.º 1 (janeiro), Universidade Católica Editora, 2018, p. 13, onde afirma a existência de "(…) *um fenómeno de crescente captura silenciosa da identidade pessoal de cada um, com um potencial lesivo, direto ou indireto, quase ilimitado do bloco de direitos fundamentais constitucionalmente reconhecido aos particulares*".

[3] Veja-se para maiores desenvolvimentos sobre os problemas que se levantam atualmente com o desenvolvimento dos meios de comunicação e das tecnologias informáticas, e, bem assim, com a necessidade de atribuir poderes de maior controle aos cidadão, a obra de Maria Leonor da Silva Teixeira, «A União Europeia e a proteção de dados pessoais: "Uma visão futurista"?», in *Revista do Ministério Público*, n.º 135, 2013.

[4] Neste sentido, veja-se o artigo 35.º da Constituição da República Portuguesa, que estabelece a proteção dos dados pessoais dos seus cidadãos, ao abrigo do princípio da segurança, que consubstancia um elemento essencial da ideia de Estado de Direito Democrático e do próprio sistema jurídico. Igualmente, este entendimento resulta do pensamento de Oliveira Ascensão, *O Direito – Introdução e Teoria Geral*, Almedina, 2005, p. 215.

cumprir voluntariamente com as suas obrigações tributárias. Com efeito, as informações e os dados pessoais são de tal magnitude que a administração tributária acaba por ter uma importância especial dentro da própria administração pública.

Contudo, ainda que se possa conceber algum grau de renúncia por parte dos cidadãos, face à necessidade de informação da administração tributária, a mesma não pode ser obtida a qualquer preço, pelo que devem encontrar o seu limite nos direitos fundamentais da intimidade e da privacidade. Por isso, o presente texto pretende debruçar-se sobre a proteção de dados no sistema tributário português, nomeadamente, as consequências decorrente da aplicação do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que aprovou o Regulamento Geral de Proteção de Dados (RGPD), analisando-se, preliminarmente, a sua aplicação ou não ao setor público, para depois nos debruçarmos em concreto sobre o seu impacto na proteção dos dados pessoais no sistema tributário, sob a perspetiva dos riscos associados[5].

1. A aplicação do Regulamento Geral de Proteção de Dados aos organismos do setor público

Antes de entrarmos no problema central, é necessário perceber se o Regulamento Geral de Proteção da Dados, resultante do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, é aplicável ao setor público, isto é, se a administração pública e em particular a administração tributária se encontram ou não abrangidas pelo referido instrumento legal, bem como se os princípios e as obrigações dele decorrente lhe são aplicáveis.

Na realidade existe a ideia ou, pelo menos, em parte do setor público foi sendo desenvolvida a ideia que os órgãos e as instituições públicas estariam isentas do cumprimento das regras impostas pelo RGPD. Essa conceção foi construída a partir da ideia que a aplicação de coimas a órgãos e a instituições pertencentes ao próprio setor público teria apenas o efeito de transferência de importâncias, referentes a coimas, de uma entidade pública para outra, sem que efetivamente deixassem tais importâncias de

[5] Para maiores desenvolvimentos sobre o tema do risco tecnológico e da sociedade de risco, vejam-se, entre outros, TERRINHA, Luís Heleno, *Direito e contingência: com e para além de Ulrich Beck, in Memoriam Ulrich Beck,* Atas do colóquio promovido pelo ICJP e pelo CIDP, em 22 de outubro de 2015; e BRITO, Miguel Nogueira de, *O admirável novo constitucionalismo da Sociedade de Risco, in Memoriam Ulrich Beck,* Atas do colóquio promovido pelo ICJP e pelo CIDP, em 22 de outubro de 2015.

ser processadas como públicas. Daqui decorrendo o argumento que a aplicação de sanções seria uma medida inócua e desprovida de qualquer nível de eficácia. A este argumento juntou-se outro, consubstanciado na isenção prevista em determinados Estados-membros, como seja a Dinamarca[6], o que levou alguns a defender a existência de um estatuto especial, que permitiria retirar o setor público da aplicação do RGPD.

Esta construção além de corresponder a um pensamento perigoso, no que se refere à desresponsabilização do Estado para com o dever de proteção de dados pessoais dos seus cidadãos, não encontra fundamento no Regulamento (UE), tanto na sua letra, como especialmente no seu espírito. Nesse sentido, não existe qualquer isenção que possa ser aplicada ao setor público, nomeadamente, quanto ao tratamento dos dados pessoais com que os vários sistemas tributários se vêm confrontados.

Em primeiro lugar, o artigo 4.º, do RGPD, inclui as autoridades públicas quer enquanto autoridades de controlo, quer como entidades processadoras de dados pessoais. Para tanto, veja-se que na definição de "responsável pelo tratamento" se faz aí logo referência a autoridade pública, como sendo responsável pela determinação "[d]*as finalidades e* [d]*os meios de tratamento de dados pessoais*"[7]. Igualmente, na definição de "destinatário" se verifica a inclusão da referência a autoridade pública como recetora de comunicações de dados pessoais, afastando apenas, no âmbito de inquéritos específicos, aquelas que possam receber dados pessoais ao abrigo do direito da União Europeia ou dos Estados-membros, o que não as afasta em absoluto da circunstância de serem destinatários de dados pessoais[8]. Por fim, a propósito da definição de "terceiro" é

[6] O RGPD prevê efetivamente que as entidade públicas possam estar isentas do seu pagamento, uma vez que aí se estipula, nomeadamente, no artigo 83.º, n.º 7, que "(…) *os Estados-Membros podem prever normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos estabelecidos no seu território"*. Assim, é ao abrigo da mencionada disposição que países como a Dinamarca podem isentar os organismos públicos da aplicação de coimas, uma vez que essa possibilidade foi deixada para decisão do legislador interno, carecendo de ser internamente legislada, mas não permite nem autoriza que daí se possa retirar a conclusão que as entidades públicas não se encontram sujeitas às regras e aos princípios do RGPD, sem prejuízo da existência de restrições na sua aplicação às entidades públicas (artigo 23.º do RGPD).

[7] Cfr. Artigo 4.º, 7), do RGPD, segundo o qual, entende-se por "«Responsável pelo Tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".

[8] Cfr. Artigo 4.º, 9), do RGPD, segundo o qual, entende-se por "«Destinatário», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos

ainda feita referência às autoridades públicas, como podendo estar autorizadas a tratar os dados pessoais[9].

Por seu lado, a sua vertente de controladora é encontrada na definição de "autoridade de controlo", que corresponde a "*uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51.º*"[10].

Nesta perspetiva, sem prejuízo das limitações impostas pelo artigo 23.º, do RGPD, as entidades públicas estão abrangidas e sujeitas aos princípios e às obrigações relativas à proteção de dados, o que resulta igualmente da circunstância do artigo 37.º, do RGPD, exigir que todas as autoridades ou organismos públicos, com exceção dos tribunais, pelo que não estão excluídas as autoridades tributárias e aduaneiras, têm obrigatoriamente de designar um encarregado da proteção de dados, o qual poderá ser responsável por várias autoridades ou organismos públicos[11].

Consequentemente, as autoridades públicas estão necessariamente abrangidas e sujeitas às obrigações que emanam do RGPD. Na realidade, a única derrogação geral, consagrada pelo legislador da União Europeia diz respeito à obrigação de designar por escrito um representante do responsável pelo tratamento na União Europeia[12], mas que é apenas aplicável aquelas que não se encontrem estabelecidas em países pertencentes à União Europeia. Assim sendo, *a contrario* resulta que as autoridades e organismos públicos, enquanto entidades responsáveis pelo tratamento de dados, estão sujeitas ao RGPD, sem prejuízo das restrições aos princípios e às obrigações do qual algumas

---

específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento".

[9] Cfr. Artigo 4.º, 10), do RGPD, segundo o qual, entende-se por "«Terceiro», a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;".

[10] Cfr. Artigo 4.º, 21), do RGPD.

[11] Cfr. Artigo 37.º, n.º 1, al. a), do RGPD, que refere que "O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que: a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional".

[12] Cfr. Artigo 27.º, n.º 2, al. b), do RGPD. Por força, do artigo 3.º, n.º 2, do RGPD, este regulamento é *aplicado "ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União*". Nesse âmbito, o identificado artigo 27.º impõe que o responsável pelos tratamentos dos dados pessoais ou o subcontratante designem por escrito um representante seu na União Europeia, mas isenta do seu cumprimento as autoridades ou organismos públicos – alínea b) do n.º 2 do artigo 27.º do RGPD.

entidades podem beneficiar, de acordo com as finalidades que perseguem, ao abrigo do disposto no artigo 23.º do RGPD.

Por último, o argumento da ineficácia da aplicação de sanções a entidades que se encontrem dentro da pessoa coletiva pública não procede, o que na prática vem sendo demonstrado pela existência de penalizações, como seja, a multa aplicada pela Comissão Nacional de Proteção de Dados (CNPD) à empresa pública de televisão – RTP, pelo que existe um precedente de penalizar órgãos, organismos, instituições ou empresas do setor publico. Isto mesmo resulta de modo claro do RGPD, quando aí se refere que os Estados-membros "*podem prever normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos*"[13]. Por isso, não restam dúvidas sobre a possibilidade de serem efetivamente aplicadas coimas às autoridades públicas pela violação dos princípios e das obrigações ao nível da proteção de dados pessoais previstas no RGPD.

Posto isto, torna-se necessário concluir que os órgãos e organizações do setor público, em todos os seus níveis, incluindo os municípios, que manifestam importantes competências tributárias, nomeadamente no que respeita ao seu poder tributário ao nível das taxas municipais, estão sujeitos a atuar em conformidade com os princípios e regras do RGPD, tal como qualquer outra organização privada, de qualquer parte do mundo, que utilize ou manipule dados sobre cidadãos na União Europeia.

2. Proteção de dados pessoais nas organizações do setor público: a administração pública tributária

As organizações e os órgãos do setor público lidam e têm um acesso privilegiado a dados pessoais que devem merecer um elevado grau de privacidade, como sejam os registos de saúde, os registos judiciais e os registos fiscais e da segurança social. Este conjunto de informação e de dados pessoais obrigam o Estado a garantir uma adequada e rigorosa confidencialidade, nomeadamente, quando é consabido que os sistemas de segurança do Estado português estão desprovidos do nível mínimo de segurança exigível à informação sensível que guardam.

Assim, impõem-se que o setor público e em particular a administração pública tributária adotem um conjunto de boas práticas de governança, para garantir a segurança e a confidencialidade das informações e dos dados pessoais que têm à sua

[13] Cfr. 83.º, n.º 7, do RGPD.

responsabilidade, os quais vão desde a identificação pessoal do titular dos dados; dos elementos do agregado familiar, que estão identificados ou serão identificáveis, bem como os respetivos dados dos seus números de identificação civil, fiscal e da segurança social; locais onde residem; bens imóveis e móveis da sua propriedade, nomeadamente os sujeitos a registo, bem como a sua localização e valor; dados e identificação das suas contas bancárias; nome das entidades comerciais ou não comerciais de que são responsáveis; rendimentos auferidos, bem como as respetivas entidades para quem trabalham; tipos de aquisição, consumos, investimentos e despesas em que incorrem, de onde pode resultar o conhecimento de hábitos de consumo, dos encargos incorridos, como sejam, com educação e saúde, a partir dos quais pode ainda resultar a identificação do estado de saúde dos titulares dos dados pessoais.

Este tipo de informação carece de uma forte proteção, porque dificilmente outra entidade pública ou privada terá um tão alargado acesso a informação pessoal do cidadão, pelo que se impõe o estabelecimento de regras rigorosas de segurança, mas também, de medidas organizativas, com vista a garantir um acesso restrito a tais dados e, bem assim, definir os casos da utilização dos dados e da forma de acesso aos mesmos, para que originem um alerta de violação de acesso a informação e a dados pessoais fora do padrão definido. Contudo, no caso do Estado português, o mesmo não se preparou adequadamente para a implementação do RGPD, pelo que aquilo que deveria ter sido preparado nos últimos dois anos – período para a preparação da aplicação de Regulamento – apenas agora o estará a tentar fazer, cuja consequência imediata é a violação dos princípios e das obrigações que resultam da nova regulamentação da proteção de dados pessoais. Estando a administração pública sujeita às obrigações decorrentes do RGPD quando processa os dados pessoais dos cidadãos, a mesma é responsável pela preparação da sua aplicação, não só ao nível da administração central, mas também ao nível das administrações regionais e locais.

3. O sistema tributário: o dilema entre o dever de pagar impostos e o direito fundamental à intimidade da vida privada

O sistema tributário português e a Constituição da República Portuguesa (CRP) reconhecem a existência de um dever dos cidadãos pagarem os impostos que sejam devidos em face da sua capacidade contributiva[14]. Por seu lado, a CRP reconhece

[14] Neste sentido, veja-se, para maiores desenvolvimentos, NABAIS, José Casalta, *O Dever Fundamental de Pagar Impostos – Contributo para a compreensão constitucional do estado fiscal*

igualmente como direito fundamental a reserva da intimidade da vida privada, quanto no texto fundamental resulta expresso que "a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar (…)"[15].

Deste conflito de normas de cariz constitucional, a jurisprudência portuguesa, mas também a jurisprudência de outros países da União Europeia, como sucede com o Tribunal Constitucional espanhol[16], já se pronunciaram acerca do conflito entre a obtenção de informação tributária e o direito à intimidade da vida privada, com evidente inclinação em favor do dever de pagar impostos e, consequentemente, em desfavor do direito à proteção dos seus dados pessoais.

4. Os limites do dever de pagar impostos em face do princípio da proporcionalidade

Em face do referido, o direito à intimidade da vida privada é limitado pelo dever de pagar impostos, isto é, a colisão de tais direitos constitucionais implica a inexistência, face à administração tributária, de um direito absoluto e incondicionado à reserva dos dados pessoais económicos dos cidadãos, pois, solução contrária, impediria a justa distribuição

---

contemporâneo, in Coleção Teses de Doutoramento, 4.ª reimpressão, Almedina, 2015. Está hoje solidificado na doutrina e na jurisprudência que o pagamento dos impostos é um dever fundamental dos cidadãos de uma determinada sociedade, enquanto suporte e garantia da existência do Estado e da prossecução dos seus fins, que *in fine* almeja garantir a dignidade da pessoa humana.

[15] Cfr. 26.º, n.º 1, da Constituição da República Portuguesa (CRP). Igualmente, já no âmbito específico da proteção de dados, resulta do artigo 35.º, n.º 6, da CRP, que "a todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional". Também, na constituição espanhola encontramos a mesma dicotomia com o dever de contribuição para os gastos públicos a estar consignada no artigo 31.º e os direitos de intimidade e de proteção a resultarem do 18.º da Constituição espanhola.

[16] É exemplificativo a decisão proferida no âmbito do Tribunal Constitucional espanhol, STC, 1.ª, de 26 de novembro de 1984 (RTC 1984\110) e as decisões subsequentes como a proferida no ATC, sala 2ª, 3.ª secção (Ar. RTC 2003\197), onde se refere expressamente "(…) *como cualquier otro derecho, encuentra sus límites en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, entre los cuales, puede citarse el deber de todos de contribuir al sostenimiento de los gastos públicos (art. 31.1 CE). En este sentido, la colisión entre el derecho fundamental a la intimidad personal y familiar (art. 18.1 CE) y el deber constitucional de contribuir a los gastos públicos (art. 31.1 CE) implica la inexistencia, frente a la Administración tributaria u otros poderes públicos, de un pretendido derecho absoluto e incondicionado a la reserva de los datos económicos del contribuyente con trascendencia tributaria o relevancia fiscal que haga inoperante el deber tributario que el art. 31.1 de la Constitución consagra, pues ello impediría una distribución equitativa del sostenimiento de los gastos públicos en cuanto bien constitucionalmente protegido*".

dos gastos públicos, os quais têm natureza de bem protegido constitucionalmente. Por isso, o debate não se deve centrar tanto entre o direito que deve prevalecer, mas antes, em face da ingerência justificada, sobre os limites e as obrigações que recaem sobre a administração tributária, nomeadamente ao abrigo do novo RGPD.

Por regra, os dados pessoais que são detidos pelas administrações públicas, em particular pela administração tributária, são processados com base numa obrigação legal ou na medida do necessário para o desempenho das atribuições e competências com natureza de interesse público (ou de exercício de autoridade pública). Os órgãos da administração tributária estão investidos tanto dessas atribuições de interesse público como de poderes de autoridade, bastando observar os poderes de investigação cada vez mais amplos da inspeção tributária ou dos poderes do diretor-geral da Autoridade Tributária no acesso a dados que tradicionalmente estavam mais severamente protegidos pelo segredo bancário[17], mas que hoje apresentam cada vez mais derrogações, para o combate à fraude fiscal internacional, ao planeamento fiscal agressivo e abusivo e para o controle de organizações criminosas e terroristas internacionais.

Tal intrusão ou ingerência não pode ser, contudo, arbitrária, mas antes deve resultar conforme ao princípio da proporcionalidade e da necessidade[18]. Por isso, em face da nova governação da informação e dos dados pessoais, a administração pública em geral, e a administração tributária em particular, devem garantir o respeito pelos princípios do tratamento da informação e dos dados pessoais conforme aos ditames da justiça e da licitude, da limitação de

[17] Segundo o artigo 63.º-B, n.ºs 1 e 2, da Lei Geral Tributária, a administração tributária pode aceder sem consentimento do contribuinte, entre outras situações, em caso de indícios da prática de crime em matéria tributária; de falta de veracidade do declarado ou quando esteja em falta declaração exigível; e de acréscimos de património não justificados, ainda que necessariamente fundamentadas, por mera decisão do diretor-geral da Autoridade Tributária, sem necessidade de prévia decisão judicial.

[18] Como reconheceu o Tribunal Constitucional espanhol, o que é diretamente transponível para o ordenamento jurídico-tributário português, "(…) *es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"* – STC, 1ª, de 10 de julho de 2000 (RTC 2000\186). Segundo a LGT (portuguesa), "*O procedimento da inspeção e os deveres de cooperação são os adequados e proporcionais aos objetivos a prosseguir* (…)" – artigo 63.º, n.º 4.

finalidades e da minimização e preservação de dados pessoais. Isto é, deve ser assegurado o princípio da justiça e da licitude, o princípio do fim do tratamento de dados pessoais e o princípio da segurança.

Neste âmbito, surge a questão do tratamento de dados decorrente do cumprimento do princípio da legalidade, de que é caso evidente o princípio da legalidade fiscal, presente no sistema tributário português[19], o qual não poderá em face do RGPD deixar de implicar modificações legislativas, com vista a garantir o cumprimento desses princípios, que implicam a definição do tipo de dados, do prazo da sua validade e de garantias apropriadas à sensibilidade dos mesmos, uma vez que deve prevalecer sobre o direito interno, decorrente do princípio da primado do direito da União Europeia[20].

Com efeito, tal é desde logo notório quando é percetível a existência de um patamar mínimo imposto pelo RGPD, que obriga por exemplo o Governo a nomear para a proteção de dados pessoais um encarregado de proteção de dados, podendo, conforme anteriormente se referiu, ser nomeado um único encarregado da proteção de dados para várias autoridades ou organismos públicos[21], sem prejuízo de se vir admitir a terceirização, quando se fala na subcontratação, o que na prática implica abrir caminho à privatização da proteção dos dados pessoais detidos pela administração pública[22].

---

[19] Segundo o artigo 103.º, n.º 3, da CRP, "Os impostos são criados por lei, que determina a incidência, a taxa, os benefícios fiscais e as garantias dos contribuintes". Acresce que o artigo 8.º, n.º 1, da LGT estabelece que "Estão sujeitos ao princípio da legalidade tributária a incidência, a taxa, os benefícios fiscais, as garantias dos contribuintes, a definição dos crimes fiscais e o regime geral das contra-ordenações fiscais". Tal princípio é ainda ampliado por força do n.º 2 do artigo 8.º da LGT à liquidação e cobrança dos tributos, incluindo os prazos de prescrição e caducidade; à regulamentação das figuras da substituição e responsabilidade tributárias; à definição das obrigações acessórias; à definição das sanções fiscais sem natureza criminal; e às regras de procedimento e processo tributário.

[20] Segundo o artigo 8.º, n.º 4, da CRP, "As disposições dos tratados que regem a União Europeia e as normas emanadas das suas instituições, no exercício das respectivas competências, são aplicáveis na ordem interna, nos termos definidos pelo direito da União, com respeito pelos princípios fundamentais do Estado de direito democrático".

[21] Como refere Guilherme da Fonseca Teixeira, op. cit., p. 30 "*A obrigatoriedade de nomeação de um encarregado de proteção de dados (…) exigirá uma adaptação por parte das entidades e empresas, quer sejam de natureza pública ou privada, ao nível da sua estrutura organizativa no sentido de promover a integração do encarregado de proteção de dados (…), de modo a que possa exercer eficazmente as suas funções de garantia do direito fundamental à proteção de dados dos cidadãos*".

[22] Neste sentido, veja-se, TEIXEIRA, Guilherme da Fonseca, *op. cit.*, p. 33, onde afirma que "*é possível verificar que a previsão da obrigatoriedade de nomeação de um encarregado de proteção de dados, (…), é uma manifestação do fenómeno de privatização de deveres estaduais de proteção que se tem vindo a verificar no Direito Administrativo* [e, também, afirmamos nós no Direito Tributário], *conferindo-se aos particulares (…) tarefas de fiscalização e verificação do cumprimento integral da legalidade que, a priori, estariam a cargo das entidades públicas, no*

Por outro lado, mostra-se necessário garantir a implementação das medidas técnicas e organizacionais apropriadas à proteção dos dados pessoais, resultantes do princípio de segurança, o que no caso da terceirização (privatização) deve implicar um especial cuidado na sua contratualização com entidades privadas. Este processo de privatização, o qual é já uma nota característica do atual sistema tributário português, uma vez que vem sendo conferido aos cidadãos e empresas cada vez mais atribuições que pertenciam ao Estado. Contudo, no caso do RGPD poder-se-á assistir a um processo de privatização de natureza distinta, uma vez que não se dá em favor do próprio titular dos dados pessoais a proteger, mas de uma outra entidade ou pessoa, que ficará responsável por todo um universo de informações e dados pessoais. Por esse motivo tais instrumentos de privatização devem conter a garantia de implementação de medidas técnicas que satisfaçam a segurança dos dados pessoais dos cidadãos, bem como promovam a existência de estruturas organizativas aptas a dar cumprimento aos princípios do RGPD, às obrigações dos responsáveis públicos pelo tratamento da informação e dos dados pessoais dos cidadãos e, ainda, aos direitos dos titulares desses mesmos dados[23].

5. A Proteção de dados pessoais: a obtenção de informação sensível pela administração tributária

No sistema tributário português, a obtenção de informação por parte da administração tributária encontra consagração legal no artigo 31.º, n.º 2, da LGT, que estabelece que "São obrigações acessórias do sujeito passivo as que visam possibilitar o apuramento da obrigação de imposto, nomeadamente a

âmbito da função administrativa do Estado – fenómeno ao qual certamente não serão alheias as considerações sobre o momento atual de crise de recursos financeiros que, inevitavelmente, influência a capacidade do agir público". Também, no mesmo sentido, vejam-se SILVA, Jorge Pereira, *Deveres do Estado de Protecção de Direitos Fundamentais*, Universidade Católica Editora, 2015, p. 731; VENTAS, Rosa Maria, HERNÀNDEZ, Ignacio [et. al.], *La Administración em tiempo de crisis: presupuestación, cumplimiento de obligaciones y responsabilidades*, Thomson Reuters, Aranzadi, 2012, pp. 1071 e ss.

[23] Por exemplo, passou a estabelecer-se que as informações e os dados pessoais, detidos por órgão público, que sejam divulgadas acidentalmente ou ilegalmente para destinatários não autorizados, ou se corrompidos, esta violação deve ser notificada à autoridade de proteção de dados, no prazo de 72 horas, após a tomada de conhecimento da violação – artigo 33.º, n.º 1, do RGPD, que estabelece que "(…) o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares".

apresentação de declarações, a exibição de documentos fiscalmente relevantes, incluindo a contabilidade ou escrita, e a prestação de informações". Com o mesmo objetivo, o artigo 59.º, da LGT, estabelece o princípio da colaboração recíproca entre os órgãos da administração tributária[24], que na perspetiva do contribuinte para com o órgão público pressupõe "(…) o cumprimento das obrigações acessórias previstas na lei e a prestação dos esclarecimentos que esta lhes solicitar sobre a sua situação tributária, bem como sobre as relações económicas que mantenham com terceiros"[25]. Isto implica que, por força da lei, pessoas singulares e coletivas estão obrigadas a facultar aos órgãos da administração tributária informação própria e de terceiros, sempre que a mesma tenha relevância tributária, o que ocorrerá sempre que a mesma tenha importância concreta para a tributação da capacidade efetiva dos contribuintes, ainda que tal utilidade seja meramente hipotética[26]. Ora, tais informações e dados pessoais, que integram as obrigações acessórias, podem ser obtidas por via das declarações que periodicamente têm de ser entregues à administração tributária, ou decorrentes de pedidos autónomos desta, ao abrigo do mencionado princípio de colaboração.

5.1. Limites impostos pela proteção da intimidade da vida privada

O primeiro limite que encontramos deriva dos dados pessoais íntimos, de cariz não patrimonial, uma vez que a administração tributária está apenas habilitada pela lei a obter e solicitar dados relacionados com o cumprimento das suas próprias obrigações tributárias ou que resultem das suas relações económicas, profissionais ou financeiras com terceiros, mas que em todo o caso tenham relevância tributária. Por isso, não têm relevância nem são admitidos pela lei o acesso a dados pessoais relativos à intimidade pessoal e familiar, pelo que se deles vierem a tomar conhecimento estão obrigados a guardar reservada e confidencialidade[27].

[24] Cfr. Artigo 59.º, n.º 1, da LGT.
[25] Cfr. Artigo 59.º, n.º 4, da LGT.
[26] Neste sentido, veja-se na jurisprudência espanhola o acórdão do Tribunal Constitucional, STS, 3ª, de 7 de junho de 2003 (RJ 2003\4014).
[27] Por isso, nos termos do artigo 63.º, n.º 5, al. c), da LGT, é legítima a falta de cooperação quando tal implique "*o acesso a factos da vida íntima dos cidadãos*".

O segundo limite é imposto às entradas no domicílio do contribuinte, enquanto local onde se desenrola a vida pessoal e familiar íntima, cuja proteção é indissociável do direito à intimidade da vida privada. É, por isso, que a Constituição da República Portuguesa reconhece no seu artigo 34.º que o domicílio é inviolável[28], bem como o artigo 63.º, n.º 5, alínea a), da LGT, estabelece que "a falta de cooperação na realização das diligências previstas no n.º 1 só será legítima quando as mesmas impliquem: a) o acesso à habitação do contribuinte". Logo, quando se torne necessário a entrada no domicílio, o órgão da administração tributária só o poderá fazer mediante autorização do contribuinte afetado ou por via de uma decisão judicial para esse efeito, em que tenha sido ponderada a proporcionalidade de tal intrusão, que deverá ser sempre fundada na sua necessidade e na adequação das circunstâncias em que deve ocorrer.

O terceiro limite resulta da confidencialidade das comunicações, que corresponde a uma importante vertente do direito à intimidade da vida privada, uma vez que corresponde a um meio relevante do conhecimento de aspetos da vida privada. Por isso, na Constituição da República Portuguesa o regime da inviolabilidade do domicílio é extensível à correspondência e aos demais meios de comunicação privada[29], bem como lhe é aplicável a proibição de todas e quaisquer ingerências por parte das autoridades públicas, com exceção dos casos expressamente previstos na lei em matéria de processo criminal[30]. Por seu lado, o legislador tributário, dando cumprimento ao imperativo constitucional estabeleceu que o acesso a informação protegida, tanto pelo segredo profissional como por qualquer outro dever de sigilo legalmente regulado, como

---

[28] Segundo o artigo 34.º, n.º 1, da CRP, "*o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis*", bem como, o n.º 2 estabelece que "*a entrada no domicílio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei*". No mesmo sentido o artigo 32.º, n.º 8, da CRP, refere que "*são nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações*".

[29] Cfr. Artigo 34.º, n.º 1, da CRP. Esta disposição legal estabelece que "(…) *o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis*". Em sentido semelhante dispõe a Constituição espanhola no seu artigo 18.º, garantindo o segredo das comunicações e, em especial, das comunicações postais e telefónicas, salvo se existir decisão judicial.

[30] Segundo o artigo 34.º, n.º 2, da CRP, "*É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal*".

sucede com as comunicações dos cidadãos, está dependente de autorização judicial[31]. Da sua articulação resulta que no âmbito da aplicação do dever de pagar imposto não está prevista a possibilidade da existência de um procedimento para acesso às comunicações do contribuinte, pelo que as intervenções judiciais com vista à necessária autorização têm em vista processos de natureza penal, ainda que de fraude fiscal, quando se entendam necessárias à investigação.

Por último, encontramos a limitação de acesso às contas bancárias, para as quais se prevê um regime especial, uma vez que a LGT estabelece que o acesso a tal informação "faz-se nos termos previstos nos artigos 63.º-A, 63.º-B e 63.º-C". A partir do momento que seja derrogado o sigilo bancário, as instituições de crédito, as sociedades financeiras e as demais entidades ficam legalmente obrigadas a permitir o acesso, quando lhes seja apresentada cópia da decisão fundamentada proferida pelo diretor-geral da Autoridade Tributária e Aduaneira, nos termos do n.º 4 do artigo 63.º-B da LGT[32]. Portanto, no que respeita ao sigilo bancário este não é um direito absoluto, podendo ser objeto de derrogação por parte da administração tributária, entre outros casos, quando existam indícios da prática de crime em matéria tributária; indícios da falta de veracidade do declarado ou esteja em falta declaração legalmente exigível; e indícios da existência de acréscimos de património não justificados[33], bem como,

[31] Nos termos do artigo 83.º, n.º 2, da LGT, "O acesso à informação protegida pelo segredo profissional ou qualquer outro dever de sigilo depende, nos termos da legislação aplicável". Portanto, a informação protegida, pelo direito à intimidade da vida provada, abrange também o segredo profissional. Assim, e no mesmo sentido, como reconhece a jurisprudência espanhola do Tribunal Constitucional "*si el secreto es obligado e incluso su violación es castigada penalmente (…) la Inspección Fiscal no puede pretender que se viole* (…)*"* - STC, 1ª, de 26 de novembro de 1984 (Ar. RTC 1984\110).

[32] Cfr. Artigo 63.º, n.º 7, da LGT.

[33] Cfr. Artigo 63.º-B, n.º 1, al. a), b) e c), da LGT. Os demais casos que permitem a derrogação do sigilo bancário resultam da necessidade de verificação de conformidade de documentos de suporte de registos contabilísticos dos sujeitos passivos de IRS e IRC que se encontrem sujeitos a contabilidade organizada ou dos sujeitos passivos de IVA que tenham optado pelo regime de IVA de caixa; da necessidade de controlar os pressupostos de regimes fiscais privilegiados de que o contribuinte usufrua; da verificação da impossibilidade de comprovação e quantificação direta e exata da matéria tributável, e, em geral, quando estejam verificados os pressupostos para o recurso a uma avaliação indireta; da verificação da existência comprovada de dívidas à administração fiscal ou à segurança social; quando se trate de informações solicitadas nos termos de acordos ou convenções internacionais em matéria fiscal a que o Estado português esteja vinculado; e quando haja a comunicação de operações suspeitas, remetidas à Autoridade Tributária e Aduaneira, pelo Departamento Central de Investigação e Ação Penal da Procuradoria-Geral da República (DCIAP) e pela Unidade de Informação Financeira (UIF), no âmbito da legislação relativa à prevenção e repressão do branqueamento de capitais e financiamento do terrorismo.

quando haja recusa da exibição de documentos bancários ou de autorização para a sua consulta, quando se trate de familiares ou terceiros que se encontrem numa relação especial com o contribuinte[34]. Para este efeito, as decisões da administração tributária não são livres e incondicionadas, uma vez que o n.º 4 do artigo 63.º-B da LGT impõe que exista uma decisão fundamentada, com referência aos motivos que as justificam, bem como a competência para a sua decisão é limitada ao diretor-geral da Autoridade Tributária e Aduaneira ou aos seus substitutos legais, sem possibilidade de delegação[35].

Em síntese, nesta matéria importa estabelecer alguns limites, uma vez que o acesso indiscriminado poderá revelar dados pessoais íntimos, sem interesse para a realidade tributária, pelo que se impõe que a administração tributária adote algumas cautelas para diminuir tal risco. É por esta razão que existe a necessidade de autorização de um específico órgão superior da hierarquia da administração tributária, bem como, não se admite autorizações indeterminadas, uma vez que as operações objeto de investigação devem constar da sua fundamentação, tal como os contribuintes afetados e o período temporal a que se reporta. Igualmente, merece ter em consideração o dever de sigilo que recai sobre quem tenha conhecimento, em razão do seu cargo, sobre os dados pessoais obtidos no âmbito de investigações ou inspeções, os quais devem assegurar a manutenção do necessário segredo. Tal é fundamental para que existe um grau de confiança elevado nos funcionários e nas autoridades públicas, que no cumprimento das suas obrigações legais acedem a dados de natureza especialmente sensível, que sendo violado colocaria em causa a própria ideia de Estado de Direito Democrático.

5.2. Limites impostos pela proteção de dados pessoais

As intromissões mais graves que podem ser praticadas pela administração tributária decorrem daquelas que afetem a intimidade da vida privada, ou seja, o núcleo da vida que o individuo tem o direito de manter

[34] Cfr. Artigo 63.º-B, n.º 2, da LGT.

[35] Com exceção ao referido, o artigo 63-B, n.º 13, da LGT, estabelece que, quando se trate de informações solicitadas nos termos de acordos ou convenções internacionais em matéria fiscal a que o Estado português esteja vinculado, não há lugar a notificação dos interessados nem a audição prévia do familiar ou terceiro quando o pedido de informações tenha caráter urgente ou essa audição ou notificação possa prejudicar as investigações em curso no Estado ou jurisdição requerente das informações e tal seja expressamente solicitado por este Estado ou jurisdição.

reservado do conhecimento e da ação de terceiros. Neste âmbito, é perante a administração tributária que ocorrem as maiores possibilidades de serem afetados, porque grande parte dos dados mais sensíveis são do seu conhecimento direto ou indireto. Deste ponto de vista, é de particular importância a regulação da proteção dos dados pessoais que se encontram à guarda (responsabilidade) da administração tributária, pelo que o RGPD assume uma especial importância, embora nos pareça óbvio que a regulamentação sobre a obtenção e tratamento dos dados não possa ser a mesma que é imposta a um particular que pretenda servir-se deles para interesses comerciais, uma vez que a administração tributária atua na defesa do interesse público e sob poderes de autoridade.

Existem, portanto, particularidades a ter em conta na aplicação do RGPD à administração tributária, desde logo, porque esta goza de determinados privilégios, resultantes do dever de pagar impostos, mas que não a isenta do cumprimento das regras e dos princípios respeitantes ao tratamento dos dados pessoais, sem prejuízo de algumas limitações das quais é beneficiária.

5.2.1. A obtenção de dados pessoais: consentimento e informação

Os dados pessoais compreendem ao abrigo da RGPD a toda a "informação relativa a pessoa singular identificada ou identificável (…)"[36]. Com efeito, é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, por recurso a distintos identificadores, como sejam, um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiologia, genética, mental, económica, cultural ou social dessa pessoa singular[37].

A RGPD parte da ideia, como regra geral, da necessidade de existir o consentimento para o tratamento dos dados pessoais, resultando do artigo 6.º que "o tratamento só é licito se e na medida em que se verifique [que] (…) o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas". Porém, o mesmo é excecionado para a administração

[36] Cfr. Artigo 4.º, a), da RGPD.
[37] Sobre o conceito de identificada ou identificável veja: CORDEIRO, A. Barreto Menezes, *Dados Pessoais: conceito, extensão e limites*, Blook, 2018, disponível em http://blook.pt/publications/publication/e38a9928dbce/.

pública, nomeadamente, para a administração tributária, sendo igualmente lícito o tratamento que resulte da necessidade de dar cumprimento a uma obrigação jurídica a que o responsável do tratamento esteja sujeito, não se aplicando aqui o expresso consentimento referido. O mesmo sucederá nas situações em que o tratamento é necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, como sucede com a administração tributária[38]. Nestas situações o Estado pode manter ou aprovar normas legais mais específicas, com o escopo de adaptar a aplicação das regras do RGPD, nomeadamente, concretizando os requisitos do tratamento e outras medidas destinadas a garantir a licitude e a legalidade do tratamento[39]. Para tanto, o fundamento jurídico do tratamento ao abrigo dessas condições é definido tanto pelo direito da União Europeia como pelo direito interno[40].

Tal é lógico, pois se fosse obrigatório que a administração tributária obtivesse tal consentimento ficaria comprometida a viabilidade do funcionamento do sistema tributário e das tarefas que lhe estão atribuídas, por ficar dependente da vontade dos obrigados tributários. Estas exceções ao regime geral, em favor das administrações públicas, decorrem ainda das limitações constantes do RGPD aos direitos estabelecidos nos artigos 12.º a 22.º e 34.º, bem como aos princípios do artigo 5.º, em que se admite que possam ocorrer por medida legislativa, desde que respeitem a essência dos direitos e liberdades fundamentais e constituam uma medida necessária e proporcionada numa sociedade democrática para assegurar "outros objetivos importantes do interesse público geral (…), nomeadamente um interesse económico ou

[38] Cfr. Artigo 6.º, n.º 1, al. c) e e) da RGPD – "O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: (…) c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; (…) e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento".

[39] Cfr. Artigo 6.º, n.º 2, da RGPD.

[40] Cfr. Artigo 6.º, n.º 3, do RGPD, segundo o qual "A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.º 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido".

financeiro importante (…), incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social"[41].

5.2.2. A qualidade dos dados pessoais

O facto de a administração tributária não precisar do consentimento do afetado para a recolha e tratamento dos seus dados pessoais não significa que a administração tributária possa recolher e tratar quaisquer dados. As administrações públicas e, portanto, também, a administração tributária, estão sujeitas às obrigações legais impostas quanto à qualidade dos dados pessoais. Na realidade, resulta do artigo 5.º, da RGPD, que os dados pessoais devem ser "*adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»)*"[42], uma vez que mesmo abrangida pela possibilidade de limitação consagrada no artigo 23.º, da RGPD, tal não será admissível quando não sejam respeitados os direitos e liberdades fundamentais, bem como o princípio da proporcionalidade.

É necessário a compatibilização com a finalidade que justifica a sua obtenção, o que deve ocorrer a todo o tempo, quer no momento inicial em que se verifica a sua obtenção, quer no momento subsequente do seu tratamento. No momento da sua obtenção impõe-se, por um lado, que os dados sejam potencialmente pertinentes ou necessários, e que, por outro lado, não sejam manifestamente excessivos ou supérfluos. Já no momento do seu tratamento, impõe-se que os dados não possam ser utilizados para finalidades incompatíveis com aquelas que presidiram ao escopo da sua obtenção, devendo, inclusive, tais dados ser eliminados quando deixem de ser pertinentes ou necessários para a sua finalidade inicial.

Por fim, os dados pessoais devem assumir-se como verdadeiros, no sentido de serem exatos e atuais, de forma a que respondam à necessidade de dar cumprimento ao princípio da verdade material, que faz parte dos princípios fulcrais do sistema tributário

---

[41] Cfr. Artigo 23.º, n.º 1, al e), da RGPD. A aplicação desta norma legal é especificamente aplicável à administração tributária, excecionando a aplicação dos princípios relativos ao tratamento de dados pessoais; direitos do titular dos dados, como seja, a transparência e regras para o exercício dos direitos dos titulares dos dados; a informação e acesso aos dados pessoais; as informações a facultar quando os dados pessoais não são recolhidos junto do titular; o direito de acesso do titular dos dados; o direito de retificação; o direito ao apagamento dos dados; o direito à limitação do tratamento; a obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento; o direito de portabilidade dos dados; o direito de oposição; as decisões individuais automatizadas, incluindo definição de perfis; e a comunicação de violação de dados pessoais ao titular dos dados.

[42] Cfr. Artigo 5.º, n.º 1, al. c), do RGPD.

português, pelo que estando incorretos e incompletos devem ser modificados e completados.

5.2.3. Acesso aos dados pessoais

O direito de acesso do titular dos dados pessoais é reconhecido pelo artigo 15.º, da RGPD. Assim, sem prejuízo da possibilidade de introdução de limitações por força do artigo 23.º, o titular dos dados tem o direito de obter confirmação de que os dados pessoais que lhe digam respeito são ou não objeto do tratamento e, bem assim, caso sejam objeto de tratamento, o direito de aceder aos mesmos e a um conjunto de informações que lhes estão associadas[43].

5.2.4. Retificação e cancelamento de dados pessoais

O artigo 16.º, do RGPD, estabelece o direito de o titular dos dados pessoais obter, de forma célere, a retificação dos dados pessoais inexatos que lhe digam respeito. Igualmente, de acordo com as finalidades do tratamento, o mesmo tem ainda direito a que os dados que estejam incompletos sejam completados. Por seu lado, nos termos do artigo 17.º, do RGPD, o titular dos dados tem direito ao apagamento (cancelamento ou esquecimento) dos seus dados pessoais, nomeadamente, aqueles que deixem de ser necessários para as finalidades que motivaram a sua recolha e tratamento[44].

Contudo, não é aplicável o direito ao apagamento em determinadas situações, mostrando-se especialmente relevantes para a administração tributária a hipótese excecionada do cumprimento de uma obrigação legal que exija o tratamento, bem como a que seja consequência do exercício de funções de interesse público ou do exercício da autoridade pública de que esteja investido o responsável pelo

[43] Segundo o artigo 15.º, n.º 1, da RGPD, essas informações dizem respeito às finalidades do tratamento dos dados; às categorias dos dados pessoais; aos destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados; ao prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; à existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; ao direito de apresentar reclamação a uma autoridade de controlo; às informações disponíveis sobre a origem desses dados; e sobre a existência de decisões automatizadas.

[44] Outras das situações previstas para o exercício do direito ao esquecimento são: a retirada do consentimento e a inexistência de outro fundamento jurídico para o referido tratamento; oposição ao tratamento e não existirem interesses legítimos prevalecentes que o justifiquem; o tratamento ilícito dos dados; para cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro; e terem os dados sido recolhidos no contexto da oferta de serviços da sociedade da informação.

tratamento[45]. Logo, o apagamento dos dados pessoais não irá operar perante a administração tributária, como genericamente perante a administração pública e os tribunais. Por outro lado, os responsáveis da administração tributária podem negar o exercício destes direitos de acesso, quando o mesmo constitua um obstáculo às atuações administrativas, tendentes a assegurar o cumprimento das obrigações tributárias e, em todo o caso, quando o afetado seja objeto de ações inspetivas, sem prejuízo do mesmo conhecer o estado do processo e de aceder aos documentos de um procedimento tributário em curso[46].

6. A utilização dos dados pessoais pela administração tributária

A administração tributária pode obter um profundo conhecimento da situação pessoal e íntima dos cidadãos, o que lhe permite construir em relação a cada uma delas o seu perfil económico, tanto estático como dinâmico, mas também, de um perfil pessoal e familiar muito completo.

6.1. As medidas de proteção dos dados pessoais

a) A criação de ficheiros de titularidade pública

No âmbito privado a decisão de criação de ficheiros de dados implica a existência de consentimento dos titulares dos dados pessoais, porém, no âmbito público, ao invés do referido não é suficiente a decisão individual de qualquer pessoa, nem se permite que essa criação se faça de qualquer forma, uma vez que deverá sempre existir uma norma habilitante, naturalmente de natureza pública e submetida ao controle jurisdicional, a qual dependerá sempre de uma prévia decisão administrativa como causa idónea para controlar a sua adequação.

Portanto, a criação de ficheiros de titularidade pública deve fazer-se com fundamento em disposição de caráter geral, pelo que a sua competência é exclusiva dos órgãos que dentro da administração pública tenham competência

[45] Cfr. Artigo, 17.º, n.º 3, al. b), do RGPD – "Os n.ºs 1 e 2 não se aplicam na medida em que o tratamento se revele necessário: (…) b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento".

[46] Segundo o artigo 30.º, n.º 1, do RGPD, "os documentos dos processos administrativos e judiciais pendentes podem ser consultados pelos interessados (…)".

para estabelecer tais disposições. Por outro lado, essa decisão terá de ser objeto de publicação, para garantir o adequado conhecimento dos cidadãos afetados. Estas são exigências legais rigorosas, próprias da coisa pública, que presidem a um ordenamento jurídico rígido, mas que proporcionam também segurança e estabilidade.

b) A titularidade e responsabilidade pelos ficheiros de dados pessoais

O responsável pelo tratamento de dados do ficheiro tem de adotar medidas técnicas e organizativas adequadas a garantir a segurança dos dados de natureza pessoal, de modo a evitar a sua alteração, perda ou acesso não autorizado, os quais estarão ainda sujeitos ao necessário dever de sigilo. Pois, as autoridades públicas e os seus respetivos funcionários quando tenham conhecimento da dados pessoais e informações abrangidas pela necessidade de proteção estão obrigados a guardar sigilo sobre os mesmos, cuja violação deverá ser tratada como uma infração disciplinar muito grave.

A RGPD dispõe exatamente neste sentido quando estabelece que o responsável pelo tratamento aplica "as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades"[47]. No que respeita ao dever de sigilo, o mesmo é expressamente aplicável ao encarregado de proteção de dado, quando se refere no artigo 38.º, n.º 5, da RGPD, que "está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros"[48].

Nos ficheiros automatizados, as limitações ao tratamento deverão, em princípio, ser impostas por meios técnicos, devendo, neste caso, ser indicado de

[47] Cfr. Artigo 24.º, n.º 1, da RGPD.

[48] Neste âmbito, resulta do artigo 90.º, da RGPD, que "Os Estados-Membros podem adotar normas específicas para estabelecer os poderes das autoridades de controlo previstos no artigo 58.º, n.º 1, alíneas e) e f), relativamente a responsáveis pelo tratamento ou a subcontratantes sujeitos, nos termos do direito da União ou do Estado-Membro ou de normas instituídas pelos organismos nacionais competentes, a uma obrigação de sigilo profissional ou a outras obrigações de sigilo equivalentes, caso tal seja necessário e proporcionado para conciliar o direito à proteção de dados pessoais com a obrigação de sigilo. Essas normas são aplicáveis apenas no que diz respeito aos dados pessoais que o responsável pelo seu tratamento ou o subcontratante tenha recebido, ou que tenha recolhido no âmbito de uma atividade abrangida por essa obrigação de sigilo ou em resultado da mesma".

forma clara no sistema que o tratamento dos dados pessoais está sujeito a limitações. Neste âmbito, devem estar divididos em diferentes níveis de segurança, consoante a sensibilidade da informação tratada. Assim, num nível básico devem ser previstas medidas de segurança como a criação de perfis de usuário, acessos permitidos apenas para a execução das funções atribuídas, bem como garantido um sistema de controlo de acessos. Por seu lado, deve ser aplicado um nível médio para os arquivos sobre infrações e sanções administrativo-tributárias, o que pressupõe o aumento dos níveis de segurança e de confidencialidade face ao nível básico, enquanto o nível alto deve ser reservado para os ficheiros com dados sensíveis, como a ideologia, religião, crenças, origem racial, saúde ou vida sexual, bem como aqueles que contenham dados para fins policiais, obtidos sem o consentimento dos próprios.

c) A resposta do ordenamento perante o incumprimento das obrigações de proteção e a reação perante funcionários públicos infratores

No âmbito do RGPD, quanto às autoridades públicas, dispõe o artigo 83.º, n.º 7, que "sem prejuízo dos poderes de correção das autoridades de controlo nos termos do artigo 58.º, n.º 2, os Estados-Membros podem prever normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos estabelecidos no seu território". Portanto, a aplicação de coimas aos órgãos da administração tributária fica na disponibilidade do Estado português querer ou não legislar no sentido da punibilidade das entidades públicas, sem prejuízo da possibilidade dos seus funcionários poderem ser sancionados, nomeadamente, em caso de violação do dever de sigilo.

Esta circunstância já hoje se encontra consagrada no ordenamento jurídico português, desde logo, resultando do Código de Conduta da Autoridade Tributária e Aduaneira a imposição de uma conduta rigorosa aos funcionários da administração tributária, no que respeita, por um lado, à observância do dever de sigilo profissional e fiscal e, por outro, ao cumprimento do princípio da finalidade, que legitima o tratamento de dados pessoais pela administração

tributária[49]. Este dever de sigilo e de confidencialidade mantem-se para os funcionários públicos mesmo após o termo do exercício das funções que justificaram o seu acesso[50]. Por isso, atualmente já resulta, e assim deverá continuar a ocorrer, que o acesso não justificado a dados pessoais dos contribuintes ou a informação tributária que beneficie do sigilo, constitui violação do dever profissional, fazendo incorrer quem o pratique em responsabilidade disciplinar[51].

Por seu lado, a ainda vigente Lei de Proteção de Dados Pessoais – Lei n.º 67/98, de 26 de outubro – estabelece no seu artigo 47.º, n.º 1, que, "quem, obrigado a sigilo profissional, nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais é punido com prisão até dois anos ou multa até 240 dias", a qual é agravada de metade dos seus limites quando o agente infrator for funcionário público, como sucederá com os funcionários da administração tributária[52].

Igualmente, no ordenamento jurídico-tributário resulta do artigo 64.º, da LGT, que os dirigentes, funcionários e agentes da administração tributária estão obrigados a guardar sigilo sobre os dados recolhidos acerca da situação tributária dos contribuintes e dos elementos de natureza pessoal que obtenham conhecimento no procedimento. Daqui resulta que o procedimento inspetivo terá de ser sigiloso, impondo que os intervenientes da administração tributária guardem sigilo sobre quaisquer factos que venham a tomar conhecimento da vida pessoal e tributária do cidadão[53]. Do seu incumprimento, isto é, da violação do segredo fiscal, resulta, quando devido a negligência, a punição a título de contraordenação, com coima de 75 a 1.500 euros, conforme dispõe o artigo 115.º

---

[49] Segundo o artigo 3.º, n.º 9, do Código de Conduta da Autoridade Tributária e Aduaneira, "*os trabalhadores devem resguardar a informação a que tenham acesso no âmbito do exercício das suas funções, em especial a que esteja protegida pelos deveres de confidencialidade ou sigilo profissional"*, esclarecendo a mesma disposição legal, que estão abrangidos *"a palavra-chave e outros meios de autenticação de acesso a sistemas informáticos ou bases de dados da AT ou de outras entidades públicas, estando os trabalhadores obrigados a manter a sua confidencialidade"*.

[50] Cfr. Artigo 3.º, n.º 9, §5, do Código de Conduta da Autoridade Tributária e Aduaneira.

[51] Cfr. Artigo 3.º, n.º 9, §6, do Código de Conduta da Autoridade Tributária e Aduaneira.

[52] Cfr. Artigo 47.º, n.º 2, da Lei 67/98, de 26 de outubro (Lei de Proteção de Dados Pessoais).

[53] Cfr. Artigo 22.º, n.º 1, do Regime Complementar do Procedimento de Inspeção Tributária e Aduaneira – "O procedimento da inspecção tributária é sigiloso, devendo os funcionários que nele intervenham guardar rigoroso sigilo sobre os factos relativos à situação tributária do sujeito passivo ou de quaisquer entidades e outros elementos de natureza pessoal ou confidencial de que tenham conhecimento no exercício ou por causa das suas funções".

do Regime Geral das Infrações Tributárias (RGIT). Por seu lado, nos termos do artigo 91.º, do RGIT, "Quem, sem justa causa e sem consentimento de quem de direito, dolosamente revelar ou se aproveitar do conhecimento do segredo fiscal (…) de que tenha conhecimento no exercício das suas funções ou por causa delas é punido com prisão até um ano ou multa até 240 dias"[54].

Portanto, resulta que a responsabilidade dos funcionários da administração tributária tanto pode operar a título de responsabilidade disciplinar, por força da aplicação do Código de Conduta da Autoridade Tributária e Aduaneira, como a titulo de responsabilidade contraordenacional ou penal, consoante o ilícito de violação do dever de segredo e de confidencialidade ocorra a título de negligência ou de atuação dolosa, sem prejuízo da possibilidade dos cidadãos afetados puderem fazer operar o regime da responsabilidade extracontratual do Estado, prevista na Lei n.º 67/2007, de 31 de dezembro.

6.2. A aplicação do sistema tributário e o uso da informação de terceiros

A administração tributária apenas pode usar a informação obtida para atividades que não sejam incompatíveis com a finalidade pela qual obteve tais dados pessoais, nomeadamente, pode usá-los para efeitos de efetivar a tributação e dar cumprimento ao dever de pagar impostos. Contudo, o uso dessa informação pode dar azo a problemas relacionados com a proteção de dados, como sucede quando se verifique a necessidade de incorporar num procedimento informação relativa a terceiros, distintas do interessado, pelo que se pode levantar a legitima duvida sobre a utilização desses dados.

Na verdade estaremos muitas vezes perante um conflito de direitos em que, por um lado, encontramos o direito à proteção dos dados pessoais de terceiros e, por outro lado, as necessidades de informação decorrentes da efetiva necessidade de dar cumprimento às obrigações legais de gestão tributária e do dever de pagar impostos, em que para efeitos de comprovação da verdade material se torna muitas vezes necessário aceder a dados pessoais de terceiros. Por regra, o direito de proteção irá ceder perante as necessidades de informação

[54] Por força do n.º 2 do artigo 91.º, o funcionário da administração tributária que revele segredo de que teve conhecimento ou que lhe foi confiado no exercício das suas funções ou por causa delas com a intenção de obter para si ou para outrem um benefício ilegítimo ou de causa prejuízo ao interesse público é punido com pena de prisão até 3 anos ou multa até 360 dias.

da administração tributária, em face do interesse público subjacente à sua atividade administrativa, embora se exija que, em face da concreta finalidade, tais dados e informações cumpram com o princípio da necessidade, da adequação e da proporcionalidade.

Por essa razão, o RGPD impõe deveres de segurança ao responsável pelo tratamento de dados pessoais, e dele não estão excecionados os órgãos e organismos públicos, no sentido que no tratamento de tais dados e informações sejam aplicadas as medidas técnicas e organizativas adequadas a assegurar um nível de segurança apropriado ao risco[55]. Estas medidas deverão basear-se nas técnicas mais avançadas, nos custos de aplicação e na natureza, no âmbito, no contexto e nas finalidades do tratamento, bem como nos riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares. Este objetivo deverá ser prosseguido conforme resulta do RGPD, pela pseudonimização e pela cifragem dos dados pessoais; pela capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; pela capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; e pela introdução de um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas.

Neste âmbito, mostra-se necessário avaliar o nível de segurança existente, que no caso do sistema tributário português será baixo, devendo ser implementadas opções técnicas, mas também, organizativas, que tenham em consideração "os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento"[56]. Desta forma, o problema da colisão de direitos poderia ser tendencialmente diminuído, uma vez que adequadas soluções técnicas e organizativas poderiam garantir a inexistência de sacrifício para o contribuinte e para os terceiros afetados, ou, quando o mesmo tenha de existir, fosse o menor possível.

[55] Cfr. Artigo 32.º, n.º 1, do RGPD.
[56] Cfr. Artigo 32.º, n.º 2, do RGPD.

Deste modo, deve ser permitido apenas o acesso aos dados que sejam indispensáveis, em que o acesso a alguns documentos ocorra apenas à vista do interessado, sem possibilidade de efetivação de cópias, limitando-se o risco de difusão ilegítima, bem como do ponto de vista organizativo interno, ser o acesso sujeito a maiores condicionamentos. Assim, seria possível garantir e proteger a reserva dos dados pessoais de terceiros, conciliando os direitos fundamentais de todos os envolvidos, contribuintes, terceiros e administração tributária.

6.3. A cedência e a comunicação de dados autorizados pela lei: tribunais e outras instituições públicas

Nos expedientes administrativos, os mesmos não só contêm dados pessoais desconexos com qualquer outra informação, como esses dados aparecem relacionados com atuações ou procedimentos relativos a terceiros, no qual podem ter um interesse legitimo e direto em conhecê-los, que, desse modo, ficará a conhecer dados e informações pessoais de outro cidadão. Por exemplo, um terceiro pode ter um interesse em conhecer benefícios fiscais que a administração tributária haja concedido a outro contribuinte.

Nestes casos, devem-se conciliar os direitos constitucionalmente reconhecidos, como seja o direito à proteção dos dados pessoais, enquanto vertente do direito à proteção da reserva da intimidade da vida privada, e o direito de acesso a arquivos e registos públicos[57]. Este último direito pretende garantir a obtenção de informação que seja necessária para que os cidadãos possam valer os seus direitos e, bem assim, para que indiretamente possam verificar a atuação legal, objetiva e transparente da administração pública[58].

[57] Segundo o artigo 268.º, n.º 2, da CRP, "Os cidadãos têm também o direito de acesso aos arquivos e registos administrativos, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas". No mesmo sentido, veja-se a Lei 26/2016, de 22 de agosto, que estabelece que todos, sem necessidade de enunciar qualquer interesse, têm direito de acesso aos documentos administrativos, o qual compreende os direitos de consulta, de reprodução e de informação sobre a sua existência e conteúdo (artigo 5.º, n.º 1), o que se insere dentro da ideia de administração pública aberta, que é, também, fundada nos princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da colaboração com os particulares.

[58] Segundo o artigo 268.º, n.º 1, da CRP, "Os cidadãos têm o direito de ser informados pela Administração, sempre que o requeiram, sobre o andamento dos processos em que sejam diretamente interessados, bem como o de conhecer as resoluções definitivas que sobre eles forem tomadas". Neste sentido, veja-se ainda, que segundo o n.º 2 do artigo 2.º, da Lei 26/2016, de 22 de agosto, "A informação pública relevante para garantir a transparência da atividade administrativa, designadamente a relacionada com o funcionamento e controlo da atividade

Contudo, o referido acesso a arquivos e documentos administrativos pode sofrer de algumas restrições, exatamente para garantir a proteção dos dados mais sensíveis, como sejam, o acesso a documentos administrativos preparatórios de uma decisão ou constantes de processos não concluídos[59]. Por seu lado, os terceiros apenas podem aceder a documentos nominativos se existir autorização escrita do titular dos dados que seja explícita e específica quanto à sua finalidade e quanto ao tipo de dados a que querem aceder, bem como, se demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, que justifique o acesso à informação[60].

Por último, ainda que seja admissível o acesso a tais dados e informações, não é permitida a utilização ou reprodução de informações em violação de direitos de autor e direitos conexos ou de direitos de propriedade industrial, nem podem ser utilizados de forma incompatível com a autorização concedida, com o fundamento do acesso, com a finalidade determinante da recolha ou com o instrumento de legalização, sob pena de responsabilidade por perdas e danos e responsabilidade criminal[61]. Porém, no âmbito tributário esse acesso deve ficar limitado apenas àquele que tenha feito parte do procedimento tributário, o que decorre da informação particularmente sensível que é do conhecimento da administração tributária, embora em determinados casos os terceiros possam dele ter conhecimento, designadamente quando manifestem um interesse relevante, como seja para prosseguimento de ação penal contra quem apresentou denúncia caluniosa à administração tributária. Portanto, no âmbito do sistema tributário português funciona a regra inversa à administração pública aberta, onde prevalece, e bem se percebe as razões, o caráter reservado, protegido e confidencial dos dados pessoais face ao acesso de terceiros.

---

pública, é divulgada ativamente, de forma periódica e atualizada, pelos respetivos órgãos e entidades".

[59] Cfr. Artigo 6.º, n.º 3, da Lei 26/2016, de 22 de agosto.

[60] Cfr. Artigo 6.º, n.º 5, da Lei 26/2016, de 22 de agosto.

[61] Cfr. Artigo 8.º, da Lei 26/2016, de 22 de agosto.

Por outro lado, no que respeita à transferência de fluxos de dados para outros organismos ou instituições públicas, deve ser admitida apenas em circunstâncias especiais, nomeadamente quando tenha por destino os tribunais ou o Ministério Público. Este último quando esteja em causa o combate ao branqueamento de capitais, ao terrorismo internacional e à perceção e investigação de esquemas de fraude fiscal. Assim, neste contexto não será exigível a obtenção de consentimento do interessado quando a comunicação tem como destino os tribunais.

Contudo, esta comunicação "cega" apenas faz sentido quando o pedido se destine a uma investigação com interesse público, isto é, para perseguir delitos que tenham conexão com a atividade desenvolvida pela administração tributária e no âmbito da competência do ministério das finanças. Porém, nem sempre será esta a situação, nomeadamente, no âmbito de processos judiciais civis, em que terceiros poderão ser os verdadeiros destinatários dos dados e informações pessoais, pelo que nestas situações não deveria haver uma aceitação "cega" por parte da administração tributária.

Nestas circunstâncias, o pedido de acesso a dados e a informação pessoal deveria ser analisado, com vista a aquilatar se os contribuintes afetados são parte do processo, pois, tratando-se de terceiros, entendemos que tais dados não deveriam desde logo ser transmitidos.

No que respeita aos contribuintes que são parte nos processos judiciais, surgem duas possibilidades. A primeira possibilidade decorre dos dados pessoais serem requeridos pelo próprio titular, ainda que indiretamente, através do tribunal, em que não se vislumbra impedimento à execução da comunicação e cedência da dados e informações pessoais, embora a administração tributária enquanto responsável pelos dados pessoais esteja adstrita a impedir que durante a transferência ou o transporte de suportes de dados os mesmos possam ser lidos, copiados, alterados ou suprimidos sem autorização. A segunda possibilidade resulta da solicitação de informações, por via do tribunal, que provenha da contraparte, em que será necessário que exista uma ponderação e valoração do tribunal para admitir tal pedido, da qual terá de resultar a existência de um despacho, sobre o qual não cabe à administração tributária vir questioná-lo.

Ao invés, já terá de ser diferente a solução nos casos em que o pedido afeta terceiros que não são parte do processo judicial, impondo-se que a administração tributária não dê cumprimento, enquanto responsável pelos dados pessoais, até ser devidamente informada pelo tribunal das razões que justificam o acesso a dados e informações de terceiros que não são parte numa disputa judicial.

7. Considerações finais

In fine, a pós-modernidade assente numa sociedade e economia digital trouxe agregada a si o problema da proteção de dados pessoais, o qual gera novos perigos, nomeadamente, quando analisado o sistema tributário português são detetados conflitos entre a necessidade de dar cumprimento ao dever de pagar impostos e certos direitos, liberdades e garantias fundamentais, como seja o direito à intimidade da vida privada, os quais devem ser devidamente preservados, mesmo que se tenha de admitir a tendência prevalência dos primeiros direitos.

É com este intuito de garantir o aprofundamento da garantia dos dados pessoais, ao nível da sua segurança, confidencialidade e integridade que surge o Regulamento Geral de Proteção de Dados, que se deve considerar aplicado aos órgãos e organismos públicos, nomeadamente, à administração tributária, sem prejuízo de a mesma beneficiar de importantes restrições no que respeita à aplicação dos princípios e das regras da proteção de dados pessoais. Contudo, está sujeita a garantir a segurança e a confidencialidade dos dados do qual é responsável, o que passa, entre outras obrigações, por ter um encarregado da proteção de dados pessoais e pela necessidade de adotar medidas organizativas com o escopo de garantir a confidencialidade dos dados pessoais.

Por último, é importante atender ao movimento de privatização da proteção de dados pessoais que se poderá dar sob a égide do RGPD, que com as diferenças apontadas dará continuação a um processo de privatização das funções tradicionais da administração tributária, o que implicará a necessidade de existência de instrumentos jurídicos rigorosos para a defesa e a garantia da informação sensível que esta entidade, como nenhuma outra, detém acerca dos cidadãos.

Referências bibliográficas

ASCENSÃO, Oliveira, *O Direito – Introdução e Teoria Geral*, Almedina, 2005.

BRITO, Miguel Nogueira de, *O admirável novo constitucionalismo da Sociedade de Risco, in Memoriam Ulrich Beck,* Atas do colóquio promovido pelo ICJP e pelo CIDP, em 22 de outubro de 2015.

CALVÃO, Filipa Urbano, *Modelo de supervisão e tratamento de dados pessoais na União Europeia: da atual Diretiva ao futuro Regulamento*, in Fórum de Proteção de Dados, Lisboa, n.º 1, 2015.

CANOTILHO, Gomes, *Direito Constitucional e Teoria da Constituição*, Almedina, 2002.

CANOTILHO, Gomes; MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, vol. I, Coimbra Editora, 2007.

CORDEIRO, A. Barreto Menezes, *Dados Pessoais: conceito, extensão e limites*, Blook, 2018, disponível em http://blook.pt/publications/publication/e38a9928dbce/

MIRANDA, Jorge; MEDEIROS, Rui, *Constituição Portuguesa Anotada*, tomo I, Coimbra Editora, 2010.

NABAIS, José Casalta, *O Dever Fundamental de Pagar Impostos – Contributo para a compreensão constitucional do estado fiscal contemporâneo*, in Coleção Teses de Doutoramento, 4.ª reimpressão, Almedina, 2015.

SILVA, Jorge Pereira, *Deveres do Estado de Protecção de Direitos Fundamentais*, Universidade Católica Editora, 2015.

SILVA, Suzana Tavares da, "O tetralemma do controlo judicial da proporcionalidade no contexto da universalização do princípio: adequação, necessidade, ponderação e razoabilidade", in *Boletim da Faculdade de Direito de Coimbra*, n.º 2, 2012.

TEIXEIRA, Guilherme da Fonseca, "Identidade e autodeterminação informacional no novo Regulamento Geral de Proteção de Dados: a inevitável privatização dos deveres estaduais de proteção", in *Católica Law Review*, volume II, n.º 1 (janeiro), Universidade Católica Editora, 2018.

TEIXEIRA, Maria Leonor da Silva, «A União Europeia e a proteção de dados pessoais: "Uma visão futurista"?», in *Revista do Ministério Público*, n.º 135, 2013.

TERRINHA, Luís Heleno, *Direito e contingência: com e para além de Ulrich Beck, in Memoriam Ulrich Beck,* Atas do colóquio promovido pelo ICJP e pelo CIDP, em 22 de outubro de 2015.

VENTAS, Rosa Maria; HERNÀNDEZ, Ignacio [et. al.], *La Administración em tiempo de crisis: presupuestación, cumplimiento de obligaciones y responsabilidades*, Thomson Reuters, Aranzadi, 2012.

A proteção de dados no direito português dos registos

Carlos Pedro Seco Lopes[1]

O X Congresso Internacional de Ciências Jurídico-Empresariais, que teve lugar na ESTG do Instituto Politécnico de Leiria, no dia 6 de dezembro de 2018, teve por tema "O RGPD e o impacto nas organizações 6 meses depois". Foi composto por 3 painéis, tendo o ora subscritor sido orador no II painel subordinado ao tema "O RGPD no setor Público".

A intervenção do aqui orador teve por tema "A proteção de dados no direito português dos registos" e procurou levar aos congressistas um pouco da experiência adquirida pelo orador enquanto membro de um grupo de trabalho criado no âmbito de um projeto piloto que foi efetuado, em parceria, pela Secretaria de Estado da Justiça, pelo IRN e pelo IGFEJ, relativamente à aplicação do RGPD no registo comercial.

A exposição começou com o enquadramento da matéria através da contextualização do Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, respeitante à proteção de dados pessoais, como uma concretização rigorosa do Direito Fundamental do cidadão europeu à sua privacidade, como estabelecido na carta da EU e decorrente de inúmera jurisprudência do Tribunal de Justiça da União Europeia (TJUE). Ainda dentro do enquadramento da matéria foi abordado em traços gerais, o que mudou com o RGPD através de vários pontos de vista: do cidadão, das entidades responsáveis pela recolha e conservação dos dados, da segurança da informação, e ainda dos pontos de vista preventivo e sancionatório.

Seguidamente foi efetuada uma exposição do caminho percorrido pelo Instituto dos Registos e do Notariado (IRN, IP) na adaptação ao RGPD, tendo por base o piloto que serviu de teste para o registo comercial. Assim, foram descritas sumariamente as várias etapas do piloto que consistiram fundamentalmente no seguinte:

- Criação de equipas RGPD – central e por entidade;

- Função da equipa: avaliação da situação existente e da sua compatibilidade ao RGPD;

[1] Conservador.

- Metodologia seguida quer no plano jurídico, quer no plano tecnológico.

No plano jurídico, explanou-se resumidamente as conclusões da equipa de trabalho do IRN, retiradas dos trabalhos efetuados no âmbito do piloto, os quais nos permitiram afastar a existência de lacunas a corrigir, bem como, conseguimos concluir pela desnecessidade de preparar especificações funcionais necessárias a qualquer desenvolvimento interno ou externo que fosse eventualmente necessário para conformar o desenvolvimento da atividade registal, nesta área funcional específica, com as exigências do RGPD.

Foram ainda enunciadas as principais premissas em que assentaram as conclusões do grupo de trabalho do piloto, analisadas à luz do cumprimento dos princípios relativos ao tratamento de dados pessoais, tais como são enunciados no artigo 5º do Regulamento, designadamente quanto ao consentimento do titular dos dados, quanto à transparência da informação, quanto ao acesso à informação, atualização e correção de dados, quanto ao esquecimento, arquivo, anonimização e especificação de alterações.

No plano tecnológico a análise e conclusões relativamente à adequação das aplicações que tramitam o registo comercial, ao RGPD ficou a cargo do IGFEJ, tendo-se referido que foi o próprio Governo Português que veio fixar os requisitos mínimos da arquitetura de segurança das redes e dos sistemas de informação, necessários ao cumprimento das exigências tecnológicas resultantes do RGPD, salientando-se que tais requisitos encontram-se determinados no anexo à Resolução do Conselho de Ministros n.º 41/2018, publicada no Diário da República, 1ª série, N.º 62, de 28 de março.

Foram ainda referidas outras medidas adotadas, como por exemplo, a contratação por parte do IRN, IP, de uma consultora especializada em recolha e tratamento de dados pessoais que efetuou uma análise, transversal a todas as áreas de registo, setores e departamentos do IRN, tendo esta consultora produzido três relatórios de que se deu uma breve nota, bem como, a contratação de uma DPO por parte do Ministério da Justiça, a quem incumbe presentemente e de forma transversal a todo o Ministério da Justiça, dar cumprimento ao preceituado nos artigos 37º a 39º do RGPD.

A exposição terminou com duas questões a ponderar *de iure constituendo* que, em jeito de desafio, o aqui orador deixou aos congressistas, a saber:

Quanto ao consentimento do titular de dados pessoais: se não se deveria ponderar a existência de uma previsão legal que estabeleça a exigência de consentimento dos titulares de órgãos de administração de sociedades comerciais, nos atos em que são designados.

Quanto ao direito ao esquecimento: se deveria existir um normativo legal que previsse a possibilidade, das pessoas singulares poderem solicitar aos serviços de registo, findo um prazo suficientemente longo após a liquidação da sociedade em causa, a limitação do acesso aos dados pessoais que lhe dizem respeito, inscritos no registo, a terceiros que demonstrem um interesse específico na consulta desses dados – Acórdão do TJUE, proferido no Proc. C-398/15 (caso Manni).

Lisboa, 10 de janeiro de 2019

Painel III – Aspetos práticos do RGPD

O RGPD no contexto laboral

Joana Carneiro[1]
Joana Janson[2]

Sumário

1. Introdução; 2. Conceitos essenciais do RGPD; 3.Alguns aspetos dos dados pessoais nas relações laborais; 4. Alguns prazos de conservação dos dados pessoais na legislação laboral; 5. Conclusão.

1. Introdução

Com a entrada em vigor do Regulamento Geral de Proteção de Dados[3] (doravante RGDP), as nossas caixas de e-mails foram invadidas com pedidos de consentimento de entidades que, se calhar, nem sequer conhecíamos. No âmbito laboral, a "febre do RGPD" tem sido similar: são celebradas dezenas de adendas aos contratos de trabalho, são fixados prazos de conservação injustificados e são recolhidos consentimentos desnecessários.

O que tem vindo a suceder nas organizações, designadamente, a nível laboral, é o facto de essas organizações não terem, em primeiro lugar, analisado a legislação laboral, antes de porem em prática o RGPD, a fim de ficarem *compliance* com o mesmo.

Para fins de gestão das relações laborais, o empregador pode tratar os dados pessoais dos seus trabalhadores dentro dos limites e condições definidos no Código do Trabalho (doravante CT), em legislação laboral avulsa e no RGPD, com as especificidades estabelecidas na Lei de Proteção de Dados.

Assim, se analisarmos a legislação laboral com a devida atenção, encontramos normas relativas aos prazos de conservação, como, por exemplo, referente ao registo de sanções disciplinares, a divulgação de informação relativa ao trabalho suplementar a estruturas de representação coletiva, registo de processos de recrutamento e documentação relativa à realização das atividades do serviço de segurança e de saúde no trabalho, entre outros.

---

[1] Sócia e Advogada da José Pedro Aguiar-Branco & Associados, SPRL.
[2] Advogada estagiária da José Pedro Aguiar-Branco & Associados, SPRL.
[3] Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Deste modo, através deste estudo, pretendemos analisar a legislação laboral vigente em corolário com o RGPD, focando-nos nas matérias relativas a dados pessoais e nos prazos de conservação já previstos e estipulados naquela, com o objetivo de dar a conhecer às organizações os mecanismos exigíveis para estarem em conformidade com a legislação laboral e, em consequência disso, com o RGPD.

2. Conceitos essenciais do RGPD

Antes de iniciarmos o estudo sobre o RGPD nas relações laborais, importa esclarecer, em primeiro lugar, alguns dos conceitos base de proteção de dados pessoais essenciais para se perceber melhor o que aqui se irá analisar. O artigo 4.º do RGPD esclarece alguns conceitos que serão úteis para o presente estudo. Assim, entende-se por:

"Dados pessoais: a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Violação de dados pessoais: uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

Dados relativos à saúde: dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde;

Consentimento do titular dos dados: uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

Definição de perfis: qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou

prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

Pseudonimização: o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;

Avaliação de impacto sobre a proteção de dados: quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais.

Proteção de dados desde a conceção e por defeito: tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas."

O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade.

Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações um procedimento de certificação, que em Portugal será aprovado pelo Instituto Português da Acreditação, I.P..

3. Alguns aspetos dos dados pessoais nas relações laborais

O artigo 88.º, n.os 1 e 2 do RGPD prevê que "Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

2.As normas referidas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho" (sublinhado nosso).

Assim, a legislação laboral, nomeadamente, o CT e a Lei n.º 102/2009, de 10 de setembro, relativa à promoção da segurança e da saúde no trabalho, já estabelece normas específicas que garantem os direitos dos trabalhadores relativamente ao tratamento dos seus dados pessoais. De uma banda, existem inúmeros prazos de conservação dos dados pessoais dos trabalhadores definidos. De outra banda, a legislação laboral esclarece, direta e indiretamente, o fim para o qual os dados dos trabalhadores são recolhidos. Assim, no caso da recolha de dados pessoais nos estritos termos da relação e da legislação laboral, o princípio da finalidade, previsto no artigo 5.º, n.º 1, al. b), do RGPD, encontra-se, desde logo, cumprido.

Repare-se que, o tratamento dos dados pessoais só é considerado lícito: quando haja a prestação do consentimento por parte do titular dos dados; quando seja necessário para a execução de um contrato no qual o titular dos dados é parte; quando seja necessário cumprir uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; quando o tratamento for necessário

para a defesa de interesses vitais do titular dos dados; quando haja um interesse vital do titular dos dados ou de outra pessoa singular; quando for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública; ou, por fim, quando o tratamento for necessário para efeito dos interesses legítimos prosseguidos legítimos prosseguidos pelo responsável pelo tratamento ou terceiros, tal como dispõe o artigo 6.º do RGPD.

No que concerne ao consentimento para o tratamento de dados pessoais, previsto no artigo 6.º, n.º1, al. a), do RGPD, este só é necessário quando não existe nenhum fim ou necessidade que justificam a realização do tratamento. Ora, nas relações laborais, o tratamento de alguns dados pessoais do trabalhador justifica-se, tanto pela execução do contrato de trabalho, como pelo cumprimento de obrigações jurídicas a que o empregador está obrigado (vide al. b), c)) do referido artigo 6.º). Assim, nas relações laborais a regra é a de que o consentimento do trabalhador não constitui fundamento de legitimidade do tratamento dos seus dados pessoais. A proposta de Lei 120/XIII[4], vista e aprovada em Conselho de Ministros em 22 de março do corrente ano (2018), apresenta duas exceções a esta regra: por um lado, refere "salvo norma legal em contrário" e, por outro lado, refere "se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador". Pensamos que podemos incluir aqui, nesta segunda exceção, por exemplo, as situações em que o empregador disponibiliza algumas benesses ou liberalidades sociais aos seus trabalhadores, que implicam a recolha de outros dados pessoais, para além daqueles que já foram recolhidos no âmbito da relação laboral, como, por exemplo, é o caso dos seguros de saúde, dos tickets infância, presentes de natal, etc.

Vejamos, então, a matéria já regulada na legislação laboral relativa à proteção de dados dos trabalhadores.

Relativamente à informação pessoal que as entidades empregadoras recolhem dos seus trabalhadores, a maior parte dessa informação serve para fins legais e obrigacionais, como, por exemplo, o pedido de indicação do número de contribuinte do trabalhador para efeitos de processamento de salário.

Ademais, o artigo 127.º do CT estipula que o empregador deverá manter atualizado um registo sobre todos os trabalhadores com indicação de, por

[4]Proposta da lei que pretende assegurar a execução, na ordem jurídica interna, do RGPD.

exemplo, nome, data de nascimento, categoria profissional, início e fim das férias, faltas que impliquem perda da retribuição ou diminuição de dias de férias, entre outras. Este registo atualizado, que contém dados pessoais dos trabalhadores, tem como causa justificativa a organização da própria entidade empregadora e a possibilidade de a entidade empregadora provar, a uma possível inspeção de que seja alvo, que está a cumprir com os tempos de trabalho dos trabalhadores, por exemplo.

O CT, no seu artigo 332.º, também obriga as empresas a um registo atualizado das sanções disciplinares dos trabalhadores, a fim de ser possível verificar o cumprimento das disposições e procedimentos legalmente aplicáveis por parte da Autoridade para as Condições do Trabalho (doravante ACT), a qual pode solicitar a consulta do referido registo.

Relativamente aos meios tecnológicos de vigilância, importa esclarecer que os sistemas de vídeo ou outros meios tecnológicos de vigilância à distância não podem ser utilizados para controlar o desempenho profissional dos trabalhadores, conforme previsto no artigo 20.º, n.º 1, do CT. Deste modo, as câmaras não devem incidir regularmente sobre os trabalhadores, o que exclui a abrangência das áreas de laboração, seja em linha de produção, armazém ou trabalho administrativo em escritório.

Assim, o tratamento de dados pessoais dos trabalhadores mediante a utilização pelo empregador de meios tecnológicos de controlo à distância só pode ser efetuado com a finalidade de proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à atividade o justifiquem. De salientar que o empregador está obrigado a informar o trabalhador sobre a existência e finalidade dos meios de vigilância. Sucede que, o artigo 21.º, n. º1 do CT refere o seguinte: “a utilização de meios de vigilância a distância no local de trabalho está sujeita a autorização da Comissão Nacional de Proteção de Dados”. Ora, com a entrada em vigor do RGPD, a função da Comissão Nacional de Proteção de Dados (doravante CNPD) passou a ser de controlar e fiscalizar o processamento de dados pessoais e não de autorizar quaisquer pedidos para obtenção da validade de tratamento de dados por quaisquer pessoas. Assim, no que respeita à existência de sistemas videovigilância, a CNPD apenas fiscaliza o cumprimento dos requisitos previstos na Lei n.º 34/2013, de 16 de maio (que estabelece o regime do exercício da atividade de segurança privada), no CT e

no RGPD; já não sendo necessário efetuar-lhe qualquer pedido de autorização, preenchimento de formulário, pagamento de taxa ou comunicação[5].

As imagens gravadas e outros dados pessoais registados através da utilização dos sistemas e equipamentos referidos no parágrafo anterior só podem ser utilizados no âmbito de processo-crime, caso em que poderão ser ainda utilizados para efeito de responsabilidade disciplinar. Assim, no caso de a infração disciplinar consubstanciar igualmente um crime, para além do processo disciplinar, a entidade empregadora deverá apresentar queixa-crime e entregar às autoridades competentes (designadamente órgãos de polícia criminal), como prova da responsabilidade criminal e disciplinar do trabalhador, o registo das câmaras de videovigilância.

Importa referir, ainda, o tratamento de dados biométricos dos trabalhadores, previsto no artigo 18.º do CT. O registo e a contagem do tempo de trabalho, através dos dados biométricos do trabalhador só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador nos casos em que haja consentimento prestado nos termos do RGPD. Tal como na situação da videovigilância, acreditamos que a necessidade de notificação à CNPD do tratamento destes dados deixará de existir, passando as entidades empregadoras a terem a obrigação de cumprirem com a finalidade de recolha dos dados biométricos e de os tratarem de forma *compliance* com o RGPD. A CNPD apenas irá averiguar se o tratamento e a recolha estão em conformidade com o RGPD, e, em caso negativo, aplicar uma coima.

O artigo 16.º do CT, relativo à reserva da intimidade da vida privada, importa: por um lado, destacar que o mesmo respeita a direitos de personalidade tanto do empregador como do trabalhador e; por outro lado, relacioná-lo com o artigo 22.º, n.º 1 do CT, que indica que "o trabalhador tem direito à reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de caráter não profissional que envie, receba ou consulte, nomeadamente através de correio eletrónico"[6]. Efetivamente, o n.º 2

[5] A este propósito, vide o site da CNPD que esclarece algumas dúvidas que surgem no âmbito do RGPD: https://www.cnpd.pt/bin/faqs/faqs.htm

[6] A este propósito *vide* Martinez, Pedro Romano, AAVV, Código do Trabalho Anotado, Almedina, 10ª Edição, 2016, pp.147 e 148: «(…) que o direito à reserva da intimidade da vida privada abrange quer o *acesso*, quer a *divulgação* de aspetos atinentes à esfera íntima e pessoal das partes, o que significa que, para além da intromissão, também a difusão de tais elementos não é permitida. Assim, mesmo nos casos em que haja consentimento por parte do trabalhador

do referido artigo 22º, cria a possibilidade de o empregador poder estabelecer regras de utilização dos meios de comunicação na empresa, por exemplo, correio eletrónico. Isto significa que, o empregador deverá estabelecer as regras de utilização de comunicação da empresa no regulamento interno da empresa[7] (artigo 99.º, CT). A elaboração deste regulamento obriga à audição, nos termos do artigo 99.º, n.º 2, do CT, da comissão de trabalhadores ou de outras estruturas representativas dos trabalhadores, caso esta não exista, e a sua produção de efeitos depende da publicitação do respetivo conteúdo e do envio para a ACT.

Previamente à definição destas normas internas, deve o empregador avaliar o impacto que as medidas de controlo pretendidas poderão ter na privacidade dos trabalhadores e, em função disso, encontrar aquelas que sejam menos intrusivas para a privacidade dos trabalhadores, e que simultaneamente satisfaçam os legítimos objetivos da organização (*Privacy Impact Assessmen*t).

Ademais, o artigo 17.º do CT prevê a impossibilidade de o empregador exigir determinadas informações (relacionadas com a vida privada, a saúde, o estado de gravidez) ao candidato a empego ou a trabalhador, de forma a proteger os dados pessoais do trabalhador. Porém, no que respeita ao "estado de gravidez", convém realçar que o artigo 36.º do CT refere que as trabalhadoras grávidas, puérpera e lactante têm que indicar, por escrito, ao empregador o seu estado. Ora, se por um lado, no artigo 17.º protege a trabalhadora de prestar essa informação, por outro lado, o artigo 36.º alude a que as trabalhadoras têm que informar o empregador do seu estado, tendo em vista ficarem abrangidas pelo regime de proteção da parentalidade.

No que concerne aos testes e exames médicos, o artigo 19.º do CT, reforça, nos n.ºs 1 e 2 que "o empregador não pode, para efeitos de admissão ou permanência no emprego, exigir a candidato a emprego ou a trabalhador a realização ou apresentação de testes ou exames médicos, de qualquer natureza, para comprovação das condições físicas ou psíquicas, salvo quando estes tenham por finalidade a proteção e segurança do trabalhador ou de terceiros, ou quando particulares exigências inerentes à atividade o justifiquem, devendo em

quanto à tomada de conhecimento pelo empregador de determinados aspetos da vida privada daquele, continua a incidir sobre o empregador o dever de os não revelar a terceiros, ou vice-versa.»

[7] *Vide* a este propósito a Deliberação n.º 1638/2013 CNPD

qualquer caso ser fornecida por escrito ao candidato a emprego ou trabalhador a respetiva fundamentação." e "O empregador não pode, em circunstância alguma, exigir a candidata a emprego ou a trabalhadora a realização ou apresentação de testes ou exames de gravidez."

Ainda a propósito dos exames de saúde, a Lei n.º 102/2009, de 10 de setembro, relativa à promoção da segurança e da saúde no trabalho, rege nos seus artigos 108.º, 109.º, 110.º questões respeitantes tanto aos exames médicos como a fichas clínicas e a fichas de aptidão[8].

As fichas clínicas e as fichas de aptidão contêm dados de saúde respeitantes aos trabalhadores. Nos termos do artigo 109.º, da Lei n.º 102/2009, a ficha clínica não deve conter dados pessoais dos trabalhadores que não estejam relacionadas com patologias ou dados de saúde. Este artigo também protege os dados pessoais dos trabalhadores na medida em que o médico responsável pela vigilância da saúde dos trabalhadores apenas entregará ao trabalhador que deixar de prestar serviço na empresa a sua ficha clínica e remete para o serviço competente na área da segurança social com competência para reconhecer doenças profissionais. Ou seja, o empregador nunca tem conhecimento do conteúdo das fichas clínicas dos trabalhadores.

Relativamente às fichas de aptidão, o empregador, também, não terá acesso às mesmas. O médico responsável preenche uma ficha de aptidão, a informar os recursos humanos da empresa, sobre se o trabalhador está apto, inapto, ou apto condicionalmente. Em suma, o empregador não terá conhecimento dos dados de saúde do trabalhador.

Além disto, cumpre não esquecer as situações de medicina preventiva. É necessário ter em consideração a proteção de dados pessoais no âmbito dos controlos de alcoolemia e consumo de droga.

No que concerne à segurança e saúde, urge, ainda, enunciar, o facto de o empregador ter a obrigação legal de transferir a sua responsabilidade pela reparação de acidentes de trabalho a entidades seguradoras, conforme previsto no artigo 283.º, n.º 5 do CT. Claro que, o empregador terá que transferir dados pessoais do trabalhador para que seja possível realizar o contrato de seguro. Neste sentido, a transferência e o tratamento de dados por parte da seguradora,

[8] O artigo 108.º menciona que devem ser realizados exames de saúde, tanto de admissão, periódicos como ocasionais.

tem como causa justificativa o cumprimento de uma obrigação legal, decorrente do CT e da LAT – Lei n.º 98/2009, de 04/09.

Uma das temáticas que surge aliada à proteção dos dados pessoais é a prevenção do assédio, regulada pela Lei n.º 73/2017, de 16 de agosto, que alterou o CT, reforçando o quadro legislativo para a prevenção da prática de assédio no contexto laboral. Agora, segundo esta alteração ao CT, as entidades empregadoras são obrigadas a gerir as comunicações internas e prevenir possíveis irregularidades. Assim, importa acautelar a proteção de dados pessoais tanto do denunciante como das possíveis testemunhas por si indicadas.

Por fim, há normas que obrigam o empregador a divulgar dados dos trabalhadores a terceiros. Desde logo, o artigo 231º, n.º 7 do CT e o artigo 3º da Portaria n.º 55/2010, de 21 de janeiro, que regula o conteúdo do relatório anual referente à informação sobre a atividade social da empresa e o prazo da sua apresentação, por parte do empregador, à ACT, referem que a empresa deve promover o visto da relação nominal dos trabalhadores que prestaram trabalho suplementar. Também o artigo 32º, da Lei n.º 105/2009[9], de 14 de setembro, que

[9] Dada a sua relevância transcrevemos aqui o teor do referido artigo 32.º, sob a epígrafe, Prestação anual de informação sobre a atividade social da empresa:
1 - O empregador deve prestar anualmente informação sobre a atividade social da empresa, nomeadamente sobre **remunerações, duração do trabalho, trabalho suplementar, contratação a termo, formação profissional, segurança e saúde no trabalho e quadro de pessoal**.
2 - A informação a que se refere o número anterior é apresentada por meio informático, com conteúdo e prazo regulados em portaria dos ministros responsáveis pelas áreas laboral e da saúde.
3 - O empregador deve dar a conhecer, previamente ao prazo constante da portaria a que se refere o número anterior, **à comissão de trabalhadores** ou, na sua falta, **à comissão intersindical ou comissão sindical da empresa,** a informação a que se refere o n.º 1, os quais podem suscitar a correção de irregularidades, no prazo de 15 dias.
4 - A informação que, de acordo com a portaria referida no n.º 2, seja prestada de modo individualizado deve ser previamente dada a conhecer aos trabalhadores em causa, os quais podem suscitar a correção de irregularidades, no prazo de 15 dias.
5 - O empregador deve proporcionar a informação aos trabalhadores da empresa e enviá-la, em prazo constante da portaria a que se refere o n.º 2, às seguintes entidades:
a) O serviço com competência inspetiva do ministério responsável pela área laboral;
b) Os sindicatos representativos de trabalhadores da empresa que a solicitem, a comissão de trabalhadores, bem como os representantes dos trabalhadores para a segurança e saúde no trabalho na parte relativa às matérias da sua competência;
c) As associações de empregadores representadas na Comissão Permanente de Concertação Social que a solicitem.
6 - **Os sindicatos e associações de empregadores podem solicitar a informação** até 10 dias antes do início do prazo para entrega da mesma.
7 - O serviço a que se refere a alínea a) do n.º 5 deve remeter a informação ao serviço do mesmo ministério competente para proceder ao apuramento estatístico da informação no quadro do sistema estatístico nacional e em articulação com o Instituto Nacional de Estatística, I. P.

regulamenta e altera o CT, estipula que o empregador deve prestar informação sobre a atividade social da empresa, por exemplo, a estruturas de representação coletiva que o solicitem e, apesar de o legislador ter tido o cuidado de obrigar à expurgação de elementos nominativos dessa informação (com exclusão do sexo, na sequência da alteração introduzida pela Lei 60/2018, 21/08), exceciona as remunerações relativamente aos sindicatos, o que pode implicar, por exemplo, que os sindicatos tenham conhecimento de salários de trabalhadores não sindicalizados contra a vontade destes.

De todo o exposto resulta que, no cumprimento de diversas obrigações legais que lhe são impostas, o empregador tem de transmitir a terceiros os dados pessoais dos seus trabalhadores.

4. Alguns prazos de conservação dos dados pessoais dos trabalhadores previstos na legislação laboral

Não há um prazo legal estatuído numa norma que defina o período máximo durante o qual os dados pessoais podem ser guardados. Assim o tratamento de dados pessoais, deverá ser efetuado sempre de acordo com os princípios que estão subjacentes ao RGPD, estatuídos no artigo 5.º do RGPD, como por exemplo, a licitude, a proporcionalidade e a finalidade pela qual são tratados. Tal significa que os dados só podem ser guardados para fins lícitos e muito bem definidos; por outro lado, os dados não podem ser guardados para além do período de tempo necessário para cumprir a finalidade que legitima a sua conservação. Além disso, a conservação deverá obedecer a uma lógica de minimização, na medida em que apenas os dados estritamente necessários para um dado fim poderão ser conservados nestes termos, limitação expressamente prevista no artigo 5.º, n.º 1, e), do RGPD.

O CT e alguma legislação laboral avulsa já estipulam alguns prazos de conservação dos dados pessoais dos trabalhadores. Apesar de existir a hipótese

8 - **A informação prestada aos representantes dos empregadores ou dos trabalhadores, com exceção das remunerações em relação aos sindicatos, e ao serviço competente para proceder ao apuramento estatístico deve ser expurgada de elementos nominativos, excluindo o sexo.**
9 - O empregador deve conservar a informação enviada durante cinco anos.
10 - Constitui contraordenação muito grave a violação do disposto no n.º 8, na parte respeitante ao empregador, contraordenação grave a violação do disposto no n.º 5 e contraordenação leve a violação do disposto nos n.os 3, 4 e 9.

de alteração dos prazos de conservação com a entrada em vigor da tão esperada *Nova* Lei de Proteção de Dados[10], que virá assegurar a execução do RGPD, ou até possíveis alterações ao CT nesta matéria, a verdade é que já estão salvaguardados os prazos de conservação de muitos dados pessoais objeto de tratamento na execução do contrato de trabalho.

Tal como já indicado neste estudo, o artigo 127.º, n.º 1, al. j), do CT, prevê que os registos dos trabalhadores devem estar sempre atualizados com o objetivo de, em primeiro lugar, provar, caso seja necessário, a uma possível inspeção por parte da ACT de que o empregador está a cumprir com os pressupostos legais impostos. Em segundo lugar, estes registos servem para facilitar a própria organização dos contraentes (empregador e trabalhador) e servem de prova das obrigações e direitos inerentes à relação laboral.

Deste modo, cessando o contrato de trabalho, consideramos que o prazo de conservação dos registos poderá ser de um ano, pois, nos termos do artigo 337.º, n.º 1 do CT, o trabalhador tem precisamente um ano, a partir do dia seguinte àquele em que cessou o contrato de trabalho, para reclamar os seus créditos laborais. Assim, e uma vez que os registos também servem para contabilizar os créditos laborais, faz sentido que os registos se conservem durante o ano seguinte à cessação do contrato de trabalho. Neste sentido, também os recibos de vencimento devem ser conservados pelo prazo de um ano a contar da cessação do contrato de trabalho, sob pena de o empregador não conseguir provar os pagamentos que efetuou dos créditos laborais que forem reclamados judicialmente pelo trabalhador. *A contrario sensu*, já é mais difícil justificar a manutenção de registos que contenham dados pessoais de ex-trabalhadores da empresa (com exceção dos casos especificamente previstos na lei) para além do referido prazo de um ano, pois neste caso o trabalhador não tem mais a possibilidade de requerer judicialmente os possíveis créditos laborais em falta.

Já no que diz respeito ao prazo dos créditos laborais relacionados com a compensação por violação do direito a férias, indemnização por aplicação de sanção abusiva ou pagamento de trabalho suplementar, dispõe o artigo 337.º, n.º 2, do CT, que aqueles que se venceram há mais de cinco anos só podem ser

[10] Daí a já referida Proposta de Lei n.º 120/XIII.

provados por documento idóneo. Daqui decorre que, em cumprimento do princípio da minimização, as empresas que destruam registos antigos (com antiguidade superior a cinco anos) referentes a esta matéria do tempo de trabalho (horário de trabalho e suas alterações, mapas de férias) de ex-trabalhadores, para além de estarem em cumprimento do RGPD dificultam a prova de tais créditos pelos ex-trabalhadores visados.

Por outro lado, também a não manutenção de bases de dados com informação de salários e descontos para a Segurança Social, poderá prejudicar essencialmente os trabalhadores (titulares dos dados), uma vez que a qualquer momento poderá ser necessário demonstrar a respetiva carreira contributiva, designadamente para efeitos de acesso à reforma dos mesmos.

No que se refere aos dados de conservação especificamente previstos na legislação laboral, destacamos as seguintes situações:

O registo dos processos disciplinares, como acima mencionámos, tem que estar sempre atualizado e justifica-se sempre no decorrer da vigência do contrato de trabalho. A partir da cessação do contrato de trabalho, a conservação deste registo poderá justificar-se durante cinco anos (337.º, n.º 2, CT), para prova da não aplicação de sanções abusivas. Também os registos de processos de recrutamento efetuados devem ser mantidos no prazo de cinco anos, com desagregação por sexo, com os elementos indicados no artigo 32.º, n. º1 do CT.

Do mesmo modo, o empregador deve manter durante cinco anos os registos dos tempos de trabalho e do trabalho suplementar, conforme previsto respetivamente nos artigos 202.º, n.º 4 e 231.º, n.º 8 do Código do Trabalho.

É também de cinco anos (nos termos do artigo 73ºB, n. º5, da Lei 102/2009[11]) o prazo de conservação de documentação relativa a avaliações de

[11] Artigo 73.º-B
"Atividades principais do serviço de segurança e de saúde no trabalho
1 - O serviço de segurança e de saúde no trabalho deve tomar as medidas necessárias para prevenir os riscos profissionais e promover a segurança e a saúde dos trabalhadores, nomeadamente:
a) Planear a prevenção, integrando, a todos os níveis e para o conjunto das atividades da empresa, a avaliação dos riscos e as respetivas medidas de prevenção;
b) Proceder à avaliação dos riscos, elaborando os respetivos relatórios;
c) Elaborar o plano de prevenção de riscos profissionais, bem como planos detalhados de prevenção e proteção exigidos por legislação específica;
d) Participar na elaboração do plano de emergência interno, incluindo os planos específicos de combate a incêndios, evacuação de instalações e primeiros socorros;
e) Colaborar na conceção de locais, métodos e organização do trabalho, bem como na escolha e na manutenção de equipamentos de trabalho;

risco profissionais, listas de acidente de trabalho, das situações de baixa por doença, das medidas propostas pelo serviço de segurança e saúde, e exames de vigilância da saúde, relatórios e as fichas, bem como registos clínicos e outros elementos informativos relativos ao trabalhador.

Contudo, o prazo de conservação dos registos e arquivos de documentos referentes a serviço de segurança e de saúde no trabalho nas situações de atividade que coloque em causa o património genético é de 40 anos, nos termos do artigo 46º, n. º3, da Lei 102/2009[12].

---

f) Supervisionar o aprovisionamento, a validade e a conservação dos equipamentos de proteção individual, bem como a instalação e a manutenção da sinalização de segurança;
g) Realizar exames de vigilância da saúde, elaborando os relatórios e as fichas, bem como organizar e manter atualizados os registos clínicos e outros elementos informativos relativos ao trabalhador;
h) Desenvolver atividades de promoção da saúde;
i) Coordenar as medidas a adotar em caso de perigo grave e iminente;
j) Vigiar as condições de trabalho de trabalhadores em situações mais vulneráveis;
l) Conceber e desenvolver o programa de informação para a promoção da segurança e saúde no trabalho, promovendo a integração das medidas de prevenção nos sistemas de informação e comunicação da empresa;
m) Conceber e desenvolver o programa de formação para a promoção da segurança e saúde no trabalho;
n) Apoiar as atividades de informação e consulta dos representantes dos trabalhadores para a segurança e saúde no trabalho ou, na sua falta, dos próprios trabalhadores;
o) Assegurar ou acompanhar a execução das medidas de prevenção, promovendo a sua eficiência e operacionalidade;
p) Organizar os elementos necessários às notificações obrigatórias;
q) Elaborar as participações obrigatórias em caso de acidente de trabalho ou doença profissional;
r) Coordenar ou acompanhar auditorias e inspeções internas;
s) Analisar as causas de acidentes de trabalho ou da ocorrência de doenças profissionais, elaborando os respetivos relatórios;
t) Recolher e organizar elementos estatísticos relativos à segurança e à saúde no trabalho.
2 - O serviço de segurança e de saúde no trabalho deve manter atualizados, para efeitos de consulta, os seguintes elementos:
a) Resultados das avaliações de riscos profissionais;
b) Lista de acidentes de trabalho que tenham ocasionado ausência por incapacidade para o trabalho, bem como acidentes ou incidentes que assumam particular gravidade na perspetiva da segurança no trabalho;
c) Relatórios sobre acidentes de trabalho que originem ausência por incapacidade para o trabalho ou que revelem indícios de particular gravidade na perspetiva da segurança no trabalho;
d) Lista das situações de baixa por doença e do número de dias de ausência ao trabalho, a ser remetida pelo serviço de pessoal e, no caso de doenças profissionais, a relação das doenças participadas;
e) Lista das medidas, propostas ou recomendações formuladas pelo serviço de segurança e de saúde no trabalho.
3 - Quando as atividades referidas nos números anteriores implicarem a adoção de medidas cuja concretização dependa essencialmente de outros responsáveis da empresa, o serviço de segurança e de saúde no trabalho deve informá-los sobre as mesmas e cooperar na sua execução.
4 - O empregador deve respeitar a legislação disciplinadora da proteção de dados pessoais.
5 - O empregador deve manter a documentação relativa à realização das atividades a que se referem os números anteriores à disposição das entidades com competência inspetiva durante cinco anos".

[12] Artigo 46.º .

Salvo melhor opinião, os processos judiciais, também, devem ser conservados pela entidade empregadora, no prazo de cinco anos, devido ao recurso extraordinário de revisão da sentença prevista no artigo 697.º, n.º 2, do CPC. Caso estejamos perante uma ação relacionada com os direitos de personalidade dos trabalhadores, os dados poderão ser conservados por tempo ilimitado, uma vez que não existe prazo máximo para se recorrer. Também nos processos emergentes de acidentes de trabalho, há sempre possibilidade de revisão de incapacidade, a qual pode ser requerida uma vez em cada ano civil (artigo 70º/3 da LAT). Deste modo, parece-nos que estes processos podem ser conservados de forma vitalícia pela empregadora, sempre que haja a sua intervenção no processo judicial.

No que concerne ao prazo de conservação das imagens de videovigilância este é de 30 dias, conforme disposto no artigo 31º, n. º2, da Lei 34/2013, de 16 de maio que estabelece o regime do exercício da atividade de segurança privada.

Por fim, a própria CNPD já se pronunciou, ainda antes da entrada em vigor do RGPD acerca de alguns prazos de conservação de dados pessoais tratados especificamente no âmbito da relação laboral:

Ora, conforme a deliberação CNPD 1638/2013[13], o prazo de conservação de dados pessoais tratados no âmbito do controlo da utilização, para fins privados, dos meios de informação e comunicação no contexto laboral é de seis meses, sem prejuízo da sua manutenção no decurso de processo disciplinar ou judicial.

"Registo, arquivo e conservação de documentos
1 - Sem prejuízo das obrigações gerais do serviço de segurança e de saúde no trabalho, em matéria de registos de dados e conservação de documentos, o empregador deve organizar e conservar arquivos atualizados, nomeadamente por via eletrónica, sobre:
a) Os critérios, procedimentos e resultados da avaliação de riscos;
b) A identificação dos trabalhadores expostos com a indicação da natureza e, se possível, do agente e do grau de exposição a que cada trabalhador esteve sujeito;
c) Os resultados da vigilância da saúde de cada trabalhador com referência ao respetivo posto de trabalho ou função;
d) Os registos de acidentes ou incidentes;
e) Identificação do médico responsável pela vigilância da saúde.
2 - Os registos a que se refere a alínea c) do número anterior devem constar de ficha médica individual de cada trabalhador, colocada sob a responsabilidade do médico do trabalho.
3 - Os registos e arquivos referidos nos números anteriores são conservados durante, pelo menos, 40 anos após ter terminado a exposição dos trabalhadores a que digam respeito".
[13] Aprovada na sessão plenária da CNPD de 16 de julho de 2013.

Relativamente ao prazo máximo de conservação dados pessoais tratados com a finalidade de medicina preventiva e curativa, no âmbito dos controlos de substâncias psicoativas efetuadas a trabalhadores, tal como definido na deliberação n.º 890/2010[14], nos termos do disposto na alínea e) do n.º 1 do artigo 5º da Lei 67/98, a CNPD fixou-o num ano, "atenta a sensibilidade dos dados pessoais objeto de tratamento". Contudo, foram excecionadas as situações de existência de processo judicial, nomeadamente decorrente de acidente de trabalho ou doença profissional, designadamente para comprovação da situação de doença.

Finalmente, no que diz respeito a penhoras de créditos salariais, também existe uma Deliberação da CNPD (n.º 923/2016) relativa ao envio de recibos de vencimento aos agentes de execução, da qual consta o seguinte: "não ser de autorizar as entidades empregadoras a facultar aos solicitadores e agentes de execução os dados pessoais constantes do recibo de vencimento dos seus trabalhadores que sejam partes em processo judicial de natureza civil". Significa isto que, da informação enviada pelas empresas aos agentes de execução, apenas deve constar a remuneração (líquida e ilíquida), devendo ficar excluído qualquer outro tipo de informação como, por exemplo, a quotização sindical, pagamentos de seguro e de pensão de alimentos, faltas ao serviço, sendo, por isso, desaconselhado o envio de recibos de vencimento que contenham tais elementos.

5. Conclusão

Após a breve análise ao impacto que o RGPD tem no contexto laboral, podemos concluir que a diversa legislação laboral existente no nosso ordenamento jurídico português já regula alguns aspetos da matéria da proteção dos dados dos trabalhadores. Por um lado, já se encontram estabelecidos prazos de conservação dos dados dos trabalhadores, sem prejuízo de novos prazos que poderão ser estabelecidos quer pela nova lei de proteção de dados quer pelas alterações à legislação laboral, que também deverá adaptar-se ao RGPD. Por outro lado, para além dos prazos de conservação, a justificação de recolha e tratamento dos dados pessoais dos trabalhadores já se encontra regulada na

[14] Aprovada em 15 de novembro de 2010.

legislação laboral. Por fim, as matérias específicas de dados pessoais que só excecionalmente se justificam no âmbito da relação laboral, como, por exemplo, o tratamento dos dados biométricos e a utilização de meios tecnológicos à distância têm sido objeto de deliberações já emanadas pela CNPD, mesmo antes da entrada em vigor do RGPD, e é precisamente relativamente a estas matérias que se justifica uma intervenção célere do legislador, pois as normas do CT estão desatualizadas face ao RGPD.

A acrescer, o trabalhador deve ter em mente que, além de titular de dados pessoais, muitas vezes é, também ele, um manuseador de dados pessoais de terceiros e, não obstante ser a empresa a entidade responsável pelo tratamento dos dados e, em alguns casos, poder haver um encarregado de proteção dos dados, o trabalhador deve contribuir para o cumprimento dos normativos legais, sob pena de infração disciplinar.

Em suma, para que as empresas estejam aptas a proceder à implementação de todas as medidas de correção para a conformidade com o RGPD no contexto laboral, importa conhecerem bem a legislação aplicável aos diversos dados pessoais dos seus trabalhadores, cujo tratamento se repute necessário para a execução do contrato de trabalho.

Por fim, recomendamos que as entidades empregadoras avaliem os tratamentos existentes (Gap Analysis), que se adaptem às novas regras do RGPD, definam a estrutura para organização dos processos e procedimentos necessários à implementação dessas regras, criem manuais e políticas internas que comprovem o cumprimento do RGPD e, se for o caso, recorram à contratação de um Data Protection Officer.

As práticas de marketing online e o tratamento de dados pessoais do consumidor menor de idade

Rute Couto, IPB [1]

Resumo: O Regulamento Geral sobre a Proteção de Dados (RGPD) estabelece as condições aplicáveis ao consentimento de crianças em relação à oferta direta de serviços da sociedade da informação, definindo a baliza etária dos 16 anos para a sua autodeterminação informacional, reduzível até aos 13 anos por iniciativa dos Estados-Membros. Numa altura em que, 6 meses depois do início de aplicação do RGPD, se discute ainda aquela redução no âmbito da proposta de lei que assegura a execução do Regulamento na ordem jurídica portuguesa, refletimos sobre o impacto do marketing online no comportamento dos menores, encarados como sujeitos autónomos e globais de direitos na sociedade da informação, com incidência nas práticas comerciais que exploram a informação pessoal recolhida junto dos consumidores menores de idade.

Palavras-chave: consumidor; menores; marketing; prática comercial.

Abstract: *The General Data Protection Regulation (GDPR) establishes the conditions applicable to child's consent in relation to the direct offer of information society services, defining the age mark of 16 years old for their informational self-determination, reducible to 13 years old by initiative of the Member States. At a time when, six months after the application of GDPR, this reduction is being discussed in the scope of the draft law that ensures the implementation of the Regulation in the portuguese legal order, we reflect on the impact of online marketing on children's behaviour, as autonomous and global subjects of rights in the information society, focusing on commercial practices that exploit personal information collected from young consumers.*

Keywords: consumer; children; marketing; commercial practice.

[1] Docente da Escola Superior de Comunicação, Administração e Turismo do Instituto Politécnico de Bragança (EsACT-IPB). Vice-Presidente da Associação Portuguesa de Direito do Consumo (apDC). Árbitro no Centro de Informação de Consumo e Arbitragem do Porto (CICAP). Doutoranda na Universidade de Santiago de Compostela.

1. Introdução: os menores como consumidores vulneráveis na sociedade da informação

A tutela da infância e juventude é um imperativo constitucional. Nos termos do artigo 69.º da Constituição da República Portuguesa (CRP), as crianças têm direito à proteção da sociedade e do Estado, com vista ao seu *desenvolvimento integral*. Já os jovens gozam de proteção especial para efetivação dos seus direitos económicos, sociais e culturais.[2] Esta tutela implica a consideração dos menores como sujeitos autónomos e globais de direitos, enquanto cidadãos e também enquanto consumidores.

Os menores atuam no mercado de consumo numa tripla qualidade[3]: diretamente, enquanto sujeitos adquirentes de bens e serviços de consumo (nos negócios jurídicos que constituem uma exceção à sua incapacidade de exercício de direitos); indiretamente, enquanto influenciadores das escolhas familiares; e potencialmente, enquanto futuros consumidores, destinatários da publicidade ou comunicação comercial e visados pelas estratégias comerciais de fidelização. As crianças estão, pois, no "epicentro da cultura de consumo".[4]

Não obstante esta posição nuclear, apresentam uma dupla *vulnerabilidade,* quando se conjuga a vulnerabilidade presumida aos consumidores em geral com a vulnerabilidade temporária inerente à menoridade.[5] Na dita sociedade da informação, contribui para o agravamento desta vulnerabilidade a "mercantilização" e "digitalização" da infância. Por um lado, pela expansão quantitativa e qualitativa do "mercado das crianças"[6] e da comunicação comercial dirigida ao público infantojuvenil quer como alvos específicos das mensagens publicitárias quer como intermediários pela sua

---

[2] Cf. artigo 70.º da CRP. A propósito da distinção entre criança e jovem, cf. JORGE MIRANDA e RUI MEDEIROS, *Constituição Portuguesa Anotada - Tomo I*, 2005, p. 711-712, e GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa - Anotada - Volume I - Artigos 1º a 107º*, 2007, p. 869-870 e 875.

[3] Cf. IGOR RODRIGUES BRITTO, *Crítica contra a publicidade infanto-juvenil brasileira*, 2007, p. 70, e MÁRIO GABRIEL DE CASTRO NUNES AZEVEDO, *Tutela do consumidor menor de idade. O consumidor menor de idade e a publicidade*, 2008, p. 70.

[4] JULIET SCHOR, cit. por DIÓGENES FARIA DE CARVALHO e THAYNARA DE SOUZA OLIVEIRA, *A Categoria Jurídica de 'Consumidor-Criança' e sua Hipervulnerabilidade no Mercado de Consumo Brasileiro*, 2015, p. 215.

[5] Cf. DIÓGENES FARIA DE CARVALHO e THAYNARA DE SOUZA OLIVEIRA, *A Categoria Jurídica de 'Consumidor-Criança' e sua Hipervulnerabilidade no Mercado de Consumo Brasileiro*, 2015, p. 219, e EKATERINE KARAGEORGIADIS, *Lanches Acompanhados de Brinquedos: Comunicação Mercadológica Abusiva Dirigida à Criança e Prática de Venda Casada*, 2014, p. 22.

[6] Cf. JAMES MCNEAL cit. por ANTÓNIO CARDOSO, *Uma perspectiva parental sobre a influência das crianças na compra de vestuário*, 2005, p. 163.

repercussão junto dos adultos. Por outro lado, porque o ambiente digital é propício à "radiação"[7] ou "cerco tentacular"[8] da publicidade.

Ao crescerem "entre ecrãs"[9] (seja televisão, computador, *smartphone*, *tablet* ou outros dispositivos), com elevado número de horas de consumo televisivo e digital, as crianças ficam sujeitas a mais estímulos publicitários. Todavia, enquanto pessoas ainda em processo de desenvolvimento biopsicológico[10], com menores competências de descodificação dos conteúdos publicitários e maior permeabilidade a influenciadores[11], são atingidas e afetadas pela publicidade de forma diversa dos adultos. Entre os impactos nocivos da publicidade dirigida a crianças ou que as afeta, o Comité Económico e Social Europeu ressalta o incitamento ao consumo excessivo conducente ao sobre endividamento, o consumo de produtos alimentares não saudáveis ou outros que se revelam nocivos ou perigosos para a saúde física e mental, o incitamento à violência ou a certos tipos de comportamentos violentos e o apelo a comportamentos sexuais excessivos.[12]

Quanto às redes sociais, jogos online e aplicações móveis, destacamos ainda um estudo da Comissão Europeia relativo ao impacto do marketing nessas plataformas sobre o comportamento das crianças.[13] Nele a Comissão analisou os mais populares jogos online, concluindo que a maioria contém publicidade, com uso de técnicas de marketing pouco transparente e sem medidas protetivas direcionadas às crianças, e que a publicidade incorporada nos jogos afeta subliminarmente o comportamento das crianças, que nem sempre reconhecem o propósito comercial dos jogos e os incentivos para fazerem compras na própria aplicação (*in-app purchase*) como forma de progresso no jogo. Por outro lado,

---

[7] Cf. SUSANA ALMEIDA, *A Publicidade Infanto-Juvenil e o Assédio pela Internet*, 2014, p. 153.

[8] Cf. CARLA AMADO GOMES, *O direito à privacidade do consumidor – A propósito da Lei 6/99, de 27 de Janeiro*, 1999, p. 103.

[9] Cf. estudos da Entidade Reguladora para a Comunicação Social disponíveis em http://www.erc.pt/pt/estudos-e-publicacoes/consumos-de-media.

[10] Cf. TAMARA AMOROSO GONÇALVES, *A regulamentação da publicidade dirigida a crianças: um ponto de encontro entre o direito da criança e do adolescente e o direito do consumidor*, 2014, p. 130.

[11] Quer à pressão social dos pares, quer aos "influenciadores digitais", tais como os *youtubers*, sobretudo na adolescência.

[12] Cf. Parecer INT/593 do Comité Económico e Social Europeu, sobre um quadro para a publicidade destinada aos jovens e às crianças, de 18 de Setembro de 2012, disponível para consulta em http://webapi.eesc.europa.eu/documentsanonymous/ces138-2012_00_00_tra_ac_pt.doc.

[13] Cf. sumário executivo, relatório final, ficha de dados e infográfico do estudo, disponíveis em https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en.

os pais entrevistados no âmbito do estudo revelaram não estar totalmente cientes dos riscos a que as crianças estão expostas no ambiente online, mostrando-se mais preocupados com a exposição dos filhos a imagens violentas e *bullying* do que com os conteúdos publicitários e a sua influência no comportamento e compras dos filhos. Além disso, as crianças não estão protegidas contra os efeitos adversos do marketing online de forma uniforme na União Europeia, quer pelas diferenças de regulação destas matérias entre Estados-Membros, quer pelas diferentes abordagens parentais de monitorização das atividades das crianças online.

2. As práticas de marketing online e a privacidade do consumidor menor de idade

A *personalização* da comunicação comercial, no desígnio de a tornar mais envolvente para os consumidores e mais valiosa para os operadores económicos, trouxe a questão para o plano da privacidade e do tratamento de dados pessoais. "Os dados são o novo ouro do século XXI, são o recurso mais valioso na economia atual, para além de serem fundamentais para a nossa vida quotidiana".[14] E as crianças de hoje têm uma "pegada digital" sem precedentes.[15]

Subjacente à proteção de dados pessoais está o direito fundamental à *autodeterminação informacional*, enquanto "direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em 'simples objeto de informações'"[16]. Mas na era da publicidade online (contextual, segmentada ou comportamental[17]), testemunhos de conexão mais ou menos

[14] Cf. artigo de opinião de Věra Jourová, Comissária responsável pela Justiça, Consumidores e Igualdade de Género, disponível em https://observador.pt/opiniao/prepararmo-nos-para-os-riscos-digitais-do-seculo-xxi/.

[15] Essa pegada digital inicia-se muitas vezes ainda enquanto nascituros (ex.: fotografia da ecografia partilhada pelos futuros pais numa rede social), continuando com toda a informação recolhida em casa (ex.: *smart toys* e monitores de vigilância parental), online (ex.: dados de navegação, partilhas nas redes sociais, aplicações) e noutros locais (ex.: dispositivos de localização, bases de dados escolares, registos médicos, entre outros), e incrementando quando o próprio menor passa a utilizar autonomamente as plataformas digitais (estima-se que ao atingir 18 anos um menor tenha feito, em média, 70 000 posts nas redes sociais). Cf. dados do estudo *"Who knows what about me?"*, promovido pelo Children's Commissioner for England, de novembro de 2018, disponível em https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/.

[16] Cf. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa - Anotada - Volume I - Artigos 1º a 107º*, 2007, p.551.

[17] Na publicidade contextual os anúncios são apresentados em função do conteúdo que a pessoa está a visualizar naquele momento. Na publicidade segmentada são selecionados com base em características fornecidas aquando do registo (ex.: género, idade, etc.). Já a publicidade comportamental implica a monitorização ao longo do tempo (ex.: sites visitados, produção de conteúdos, etc.), com vista à criação de

intrusivos, *Big Data* e *Internet of Things* (agora já *Internet of Everything*), muitos são os riscos em matéria de proteção de dados pessoais, tais como a recolha de dados sem conhecimento ou consentimento do titular, definição de perfis e exploração comercial da informação recolhida.[18]

A tutela dos consumidores menores de idade e da sua privacidade face a práticas de marketing online advinha já de outros regimes jurídicos, que complementam a proteção ora conferida pelo Regulamento. Antes de analisarmos os ditames do RGPD nesta matéria, fazemos então uma breve resenha das soluções já presentes no regime jurídico nacional:

Desde logo, o Código da Publicidade (entendida como qualquer forma de comunicação feita no âmbito de uma atividade económica com o objetivo de promover bens ou serviços) insta à proteção da *vulnerabilidade psicológica* dos menores, quando a publicidade lhes seja dirigida.[19] Do mesmo modo, o regime jurídico das práticas comerciais das empresas nas relações com os consumidores proíbe as práticas desleais, em especial as enganosas (por informações falsas ou que induzam em erro o consumidor, confusão com concorrência ou omissão de informação necessária para uma decisão esclarecida), agressivas (por limitação significativa da liberdade de escolha e comportamento do consumidor devido a assédio, coação ou influência indevida) e as "suscetíveis de distorcer substancialmente o comportamento económico de um único grupo, claramente identificável, de consumidores particularmente

perfis - Cf. Parecer 2/2010 sobre publicidade comportamental em linha, do "Grupo de Trabalho do artigo 29.º", p. 5, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_pt.pdf.

[18] A oportunidade da presente reflexão está bem patente em dois outros estudos recentes. O primeiro, da Universidade de Oxford, analisou quase um milhão de aplicações disponíveis na loja Google Play, e aferiu que as aplicações direcionadas a crianças são das mais utilizadas para recolha de dados por outras empresas (o chamado third party tracking), com implicações ao nível da definição de perfis e consentimento - Cf. Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt. 2018. Third Party Tracking in the Mobile Ecosystem. In WebSci '18: 10th ACM Conference on Web Science, May 27–30, 2018, Amsterdam, Netherlands. ACM, New York, Y, USA, 9 pages. https://doi.org/10.1145/3201064.3201089. Por outro lado, o estudo "hAPPy kids" da Universidade Católica Portuguesa evidencia que os *"digitods"*, os filhos dos primeiros "nativos digitais", que têm acesso a dispositivos digitais desde jovens, não percecionam as aplicações como perigosas e são apenas ocasionalmente supervisionados pelos pais nas suas atividades digitais – Cf. Dias, P., & Brito, R. (2018a). *Aplicações seguras e benéficas para crianças felizes. Perspetivas dos pais*. Lisboa: Centro de Estudos em Comunicação e Cultura, Universidade Católica Portuguesa e Dias, P., & Brito, R. (2018b). *Aplicações seguras e benéficas para crianças felizes. Perspetivas de famílias*. Lisboa: Centro de Estudos em Comunicação e Cultura, Universidade Católica Portuguesa. Ambos os estudos estão disponíveis na página do Católica Research Centre for Psychological, Family and Social Wellbeing (CRC-W), em https://crc-w-ucp.wixsite.com/crc-w/publicacoes.

[19] Cf. artigo 14.º do Decreto-Lei (DL) n.º 330/90 de 23 de outubro, na sua versão atual.

vulneráveis, em razão da sua doença mental ou física, idade ou credulidade, à prática comercial ou ao bem ou serviço subjacentes, se o profissional pudesse razoavelmente ter previsto que a sua conduta era suscetível de provocar essa distorção"[20], aqui se incluindo os consumidores menores de idade. A aferição do carácter leal da prática impõe que se pondere, em cada caso, se o profissional atuou sem o padrão de competência especializada e de cuidado esperado e se a prática comercial prejudicou sensível e determinantemente a aptidão do consumidor para tomar uma decisão esclarecida.[21] Todavia, o legislador dispensou desta avaliação casuística – ao inclui-la na "lista negra" das práticas comerciais consideradas *agressivas* em qualquer circunstância – a prática de "incluir em anúncio publicitário uma exortação direta às crianças no sentido de comprarem ou convencerem os pais ou outros adultos a comprar-lhes os bens ou serviços anunciados".[22]

Especificamente no que se refere aos meios digitais, o regime jurídico dos contratos à distância e fora do estabelecimento comercial proíbe expressamente a cobrança de *conteúdos digitais* não solicitados pelo consumidor[23], designadamente programas e aplicações de computador, jogos, músicas, vídeos ou textos.[24]

Por último, a lei relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas impõe o consentimento prévio (*opt-in*) do assinante ou utilizador de tais serviços quer para o armazenamento de informações e a possibilidade de acesso à informação armazenada (de que serão exemplo os *cookies* com finalidades publicitárias), quer para o envio de comunicações não solicitadas para fins de marketing direto, designadamente através da utilização de sistemas automatizados de chamada

[20] Cf. artigo 6.º a) do DL n.º 57/2008 de 26 de março, na sua versão atual. O mesmo diploma, no artigo 3.º d), define prática comercial como "qualquer ação, omissão, conduta ou afirmação de um profissional, incluindo a publicidade e a promoção comercial, em relação direta com a promoção, a venda ou o fornecimento de um bem ou serviço ao consumidor".

[21] Cf. artigo 5.º e as definições de "diligência profissional" e "distorcer substancialmente o comportamento económico dos consumidores" constantes do artigo 3º do DL 57/2008.

[22] Cf. artigo 12.º e) do DL 57/2008.

[23] Estas cobranças constituem muitas vezes o designado "WAP Billing", definido como "um mecanismo que permite aos consumidores adquirir conteúdos a partir de páginas WAP (Wireless Application Protocol), que são cobrados diretamente na fatura de serviço de acesso à Internet ou descontados no saldo (no caso dos pré-pagos)" - Cf. glossário da Autoridade Nacional de Comunicações (ANACOM), disponível em http://www.anacom-consumidor.com/glossario.

[24] Cf. artigos 3.º d) e 28.º do DL 24/2014 de 14 de fevereiro, na sua versão atual.

e comunicação que não dependam da intervenção humana, aparelhos de telecópia ou correio eletrónico, incluindo sms (serviços de mensagens curtas), ems (serviços de mensagens melhoradas), mms (serviços de mensagem multimédia) e outros tipos de aplicações similares.[25]

Nota ainda para a responsabilidade dos prestadores intermediários de serviços na sociedade da informação, de modo mais expressivo os de armazenagem principal ou em servidor (*hosting*) e, por equiparação, os de associação de conteúdos, como instrumentos de busca e hiperconexões. Apesar da ausência de um dever geral de vigilância sobre as informações armazenadas ou a que permitam o acesso, os prestadores de serviços são responsáveis, nos termos comuns, se tiverem conhecimento de atividade ou informação cuja ilicitude for manifesta e não retirarem ou impossibilitarem logo o acesso a essa informação.[26] O que, naturalmente, inclui quaisquer práticas comerciais ilícitas dirigidas a menores.

3. O tratamento de dados pessoais dos menores no âmbito do RGPD

3.1. Considerações gerais

Ainda que o tratamento de dados pessoais cujo titular seja um menor esteja na ordem do dia quanto à idade de consentimento em relação aos serviços da sociedade da informação (*age of digital consent*), impõe-se referir as demais exigências do RGPD[27] neste âmbito. Desde logo, o responsável pelo tratamento dos dados pessoais deve cumprir os princípios de tratamento de dados plasmados no artigo 5.º do RGPD, designadamente os da licitude, lealdade e transparência, limitação de finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade. Este último revela a grande mudança de paradigma operada pelo RGPD, ao instituir que o responsável pelo tratamento é responsável pelo cumprimento deste princípio e tem de poder comprová-lo (*acountability*). De um modelo de

[25] Cf. artigos 5.º e 13.º-A da Lei n.º 41/2004 de 18 de agosto, na sua versão atual.
[26] Cf. artigos 11.º a 19.º do DL n.º 7/2004 de 7 de janeiro, na sua versão atual. No caso da associação de conteúdos, o legislador estabelece que "a remissão é lícita se for realizada com objetividade e distanciamento, representando o exercício do direito à informação, sendo, pelo contrário, ilícita se representar uma maneira de tomar como próprio o conteúdo ilícito para que se remete".
[27] Muitas das quais decorriam já da Lei n.º 67/98 de 26 de outubro, que transpôs a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), revogada pelo RGPD.

hétero-regulação, assente num sistema de notificações ou controlo prévio pelas autoridades de controlo e fiscalização (em Portugal, a Comissão Nacional de Proteção de Dados), passamos para um modelo de auto-regulação, em que as organizações ficam responsáveis por garantir a observância e a contínua conformidade com o RGPD (*compliance*).

Os tratamentos de dados só são lícitos se o titular der o seu consentimento ou se for necessário para uma das finalidades previstas no RGPD, a saber: execução de um contrato ou diligências pré-contratuais; cumprimento de uma obrigação jurídica do titular dos dados; defesa de interesses vitais do titular ou de terceiros; exercício de funções de interesse público ou da autoridade pública do responsável pelo tratamento; e interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros.[28] Quando a condição de legitimidade forem tais interesses legítimos do responsável, deve ser ponderada a prevalência dos interesses ou direitos e liberdades fundamentais do titular, "em especial se o titular for uma criança".[29] Quando falamos de práticas de marketing online e do consentimento digital reportamo-nos ao primeiro daqueles fundamentos (consentimento), mas sem olvidar que pode haver tratamentos de dados pessoais de menores ao abrigo das demais hipóteses referidas (necessidade).

No âmbito dos direitos dos titulares dos dados, queremos aqui destacar três aspetos. Em primeiro lugar, o princípio da *transparência*, nos termos do qual as informações e comunicações com o titular dos dados devem ser fornecidas de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças.[30]

Em segundo lugar, o direito ao apagamento dos dados ou *"direito a ser esquecido"* se os dados deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, os titulares dos dados retirarem o consentimento ou se opuserem ao tratamento ou se os dados foram tratados ilicitamente. O artigo 17.º nº 1 f) do RGPD autonomiza neste direito ao apagamento os dados pessoais recolhidos no contexto da oferta de serviços da

[28] Cf. artigo 6.º do RGPD.
[29] Cf. alínea f) do n.º 1 do artigo 6.º do RGPD.
[30] Cf. artigo 12.º nº 1 e Considerando 58 do RGPD.

sociedade da informação, na esteira do que prevê o Considerando 65 a propósito do consentimento dado por um titular dos dados "quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento" e que pretenda, já adulto, exercer o seu direto a suprimir esses dados pessoais, especialmente na Internet, sem prejuízo do prolongamento da conservação de tais dados se revelar necessário para fins estatísticos, de interesse público, para efeitos de processo judicial, entre outros.

Em terceiro lugar, importa acautelar as crianças face à possibilidade de *definição de perfis* (*"profiling"*), definida como "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".[31] Em geral, o RGPD sujeita estas decisões individuais automatizadas a estritos requisitos, mas desde logo se especifica no Considerando 71 que "essa medida não deverá dizer respeito a uma criança".

As crianças são ainda referenciadas no RGPD enquanto pessoas singulares vulneráveis a propósito dos riscos para os direitos e liberdades resultantes de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais.[32] Por último, nas atribuições das autoridades de controlo, a propósito da promoção da sensibilização e a compreensão do público relativamente aos riscos, regras, garantias e direitos associados ao tratamento, o RGPD prevê ainda que as "atividades especificamente dirigidas às crianças" sejam alvo de uma atenção especial.[33]

3.2. Idade de "consentimento digital"

Quando a licitude do tratamento de dados pessoais se fundamente no consentimento, e no que respeita à oferta direta de serviços da sociedade da informação às crianças, o artigo 8.º do RGPD estabelece que tratamento só é lícito se o menor tiver pelo menos 16 anos, idade abaixo da qual o consentimento

[31] Cf. artigo 4.º 4) do RGPD.
[32] Cf. Considerando 75 do RGPD.
[33] Cf. artigo 57.º nº 1 b) do RGPD.

terá de ser dado ou autorizado pelos titulares das responsabilidades parentais. O próprio Regulamento prevê que os Estados-Membros possam definir uma idade inferior para o efeito, desde que igual ou superior a 13 anos.

O Parlamento Europeu e o Conselho justificam esta especial proteção especial com o facto de as crianças poderem estar "menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais" e frisando, no Considerando 38 do RGPD, que tal proteção deverá ser aplicada, nomeadamente, "à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças".

Três precisões se impõem quanto à aplicabilidade do artigo 8.º do RGDP. A primeira é a de que o normativo se refere apenas às hipóteses em que a licitude do tratamento de dados resulta do *consentimento* do titular dos dados (alínea a) do artigo 6.º do RGPD), não se aplicando às demais condições de legitimidade constantes das alíneas b) a f) do mesmo artigo 6.º A segunda é que as condições aplicáveis ao consentimento aqui definidas dizem respeito à oferta de *serviços da sociedade da informação* às crianças e não a todos os tratamentos de dados pessoais de menores. Por serviço da sociedade da informação entende-se "qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços".[34] A terceira é que só será aplicável quando haja *oferta direta* de tais serviços às crianças, excluindo as situações em que o prestador do serviço expressamente informe os potenciais utilizadores de que "só oferece

[34] Cf. artigo 1.º n.º 1 b) da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação, aplicável por remissão do artigo 4.º 25) do RGPD. Para efeitos desta definição, entende-se por "à distância" um serviço prestado sem que as partes estejam simultaneamente presentes, "por via eletrónica" um serviço enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos, e "mediante pedido individual de um destinatário de serviços" um serviço fornecido por transmissão de dados mediante pedido individual. No anexo I da Diretiva figura uma lista indicativa dos serviços não incluídos nesta definição.

os seus serviços a pessoas com 18 anos ou mais e se este facto não for refutado por outros elementos de prova".[35]

A restrição etária foi polémica, com muitas organizações ligadas à educação e proteção da criança a pronunciarem-se no sentido de que a necessidade de consentimento parental até aos 16 anos, para além de ineficaz, desconsidera os direitos dos jovens e prejudica a inclusão e literacia digital.[36] Por outro lado, a falta de harmonização entre Estados-Membros (ao permitir que a idade de consentimento varie entre os 13 e os 16 anos) contraria os propósitos da escolha do Regulamento como instrumento legislativo nesta matéria.

Segundo os dados mais recentes[37], dos 22 Estados-Membros (EM) da União que já aprovaram legislação de implementação do artigo 8.º do RGPD, as opções dos legisladores nacionais são diversas, entre os que definem os 13 anos (7 EM[38]), 14 anos (5 EM[39]), 15 anos (1 EM[40]) e 16 anos (9 EM[41]). Entre os 6 EM que ainda não aprovaram a legislação, as propostas legislativas variam entre os

[35] Cf. orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, do Grupo de Trabalho do Artigo 29.º (WP259 rev.01), p. 28, disponível em https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, adiante WP259.

[36] Destacamos a iniciativa "GDPR Have Your Say", direcionada para preparar as crianças e adolescentes, defender os seus direitos, bem como fomentar a participação dos próprios jovens, entre nós dinamizada pelo "Projeto MiudosSegurosNa.Net". Para além de um "Manual de Ação para Jovens" e outras iniciativas de participação, a equipa preparou uma lista de "10 razões pelas quais os adolescentes não precisam de consentimento parental para aceder aos serviços da sociedade de informação", subscrita pela Associação Nacional de Professores de Informática, Associação Portuguesa para a Promoção da Segurança da Informação, Associação de Professores de Filosofia, Associação D3 - Defesa dos Direitos Digitais, Aventura Social, Centro de Investigação em Artes e Comunicação, Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito de Lisboa, Confederação Nacional Independente de Pais e Encarregados de Educação, Cyprus Neuroscience and Technology Institute, Confederação Nacional das Associações de Pais, Cyberethics, Dream Teens, European Parents Association, EU Kids Online Portugal, Insight - Education to Empower, Instituto de Apoio à Criança, InternetSegura.pt, MiudosSegurosNa.Net, Narodni Centrum Bezpečnějšiho Internetu, Ora De Net, PantallasAmigas, RadioActive101 – Portugal, Safenet.bg, SaferInternet.gr, SaferInternet.pl, Safer Internet Centre Nederland, Salvati Copiii - Save the Children Romania, Sociedade Portuguesa de Medicina do Adolescente, SoMe – Right, Suradnici u Učenju, Telefono Azzurro e The Diana Award. Pela sua pertinência, aqui elencamos essas razões: 1) Respeitando os Direitos da Criança; 2) Ouçamos os investigadores do desenvolvimento; 3) Autonomia – uma área essencial do crescimento; 4) Equilibrando riscos e oportunidades; 5) Reduzindo o fosso digital; 6) Oportunidades de inclusão ou discriminação cultural?; 7) Abrindo caminho para a literacia do século XXI; 8) Cidadania global limitada pelas fronteiras nacionais; 9) Eurocrata, burocrata ou hipócrita?; 10) O direito a ser ouvido!.

[37] Cf. dados recolhidos pela Plataforma "Better Internet for Kids", disponíveis em https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751.

[38] Bélgica, Dinamarca, Finlândia, Letónia, Malta, Suécia e Reino Unido.

[39] Áustria, Chipre, Itália, Lituânia e Espanha.

[40] França.

[41] Croácia, Alemanha, Hungria, Irlanda, Luxemburgo, Holanda, Polónia, Roménia e Eslováquia.

13 anos (2 EM[42]), 14 anos (1 EM[43]) e 15 anos (3 EM[44]), sendo que até à aprovação da legislação definitiva, vigora a idade de 16 anos prevista no RGPD.

Em Portugal, a proposta de lei 120/XIII[45], que assegura a execução do RGPD na ordem jurídica nacional, no seu artigo 16.º, prevê os 13 anos como idade de acesso das crianças, sem carecer de consentimento dos seus representantes legais, à oferta direta de serviços da sociedade da informação. Mais estabelece que caso a criança tenha idade inferior a 13 anos, a licitude do tratamento depende do consentimento dos seus representantes legais, preferencialmente com recurso a meios de autenticação segura, como o Cartão de Cidadão ou a Chave Móvel Digital.

Na exposição de motivos da proposta pode ler-se simplesmente que se considera "adequada a idade de treze anos, em harmonia com a opção feita noutros Estados-Membros da União Europeia quanto a redes e plataformas que, em regra, têm um caráter transnacional", parecendo remeter a questão para o plano da harmonização, quando na realidade não foi essa a opção de mais de dois terços dos Estados-Membros.

Em contributos à proposta de lei[46], algumas entidades referiram-se à definição da idade-limite de 13 anos, nos termos que ora resumimos:

A *Comissão Nacional de Proteção de Dados* (CNPD), no seu Parecer 20/2018 assinala precisamente que o argumento expresso na exposição de motivos não se afigura decisivo, face ao propósito do legislador europeu de não homogeneizar este aspeto do regime, admitindo soluções diferenciadas em função "da idade tida como relevante em cada ordenamento jurídico para decisões sobre a sua vida". A CNPD avança ainda com a proposta de tomar por referência o critério fixado quanto ao consentimento como causa de exclusão da ilicitude penal (16 anos).[47]

---

[42] Estónia e Portugal.
[43] Bulgária.
[44] República Checa, Grécia e Eslovénia.
[45] Cf. detalhes da iniciativa no sítio da Assembleia da República, em http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368
[46] Todos os contributos, bem como as audições promovidas e propostas de alteração dos diferentes partidos políticos, estão disponíveis na página supra indicada. Aquando da entrega do presente texto, as notícias indicam que a versão final da proposta portuguesa, prevista para março de 2019, incluirá antes os 16 anos como idade mínima de consentimento digital.
[47] Este argumento é rebatido pela Associação dos Operadores de Comunicações Eletrónicas, para quem esta analogia não procede porquanto existe "uma diferença material muito significativa entre consentir em

Também a *Confederação Empresarial de Portugal* se pronunciou no sentido de que a proposta "além de não acautelar a segurança dos menores no acesso aos meios informáticos e na sociedade da informação, contraria aquilo que é a visão do legislador português relativamente à capacidade dos menores, prevista no Código Civil", onde todas as exceções à incapacidade dos menores se reportam à idade mínima dos 16 anos. Idêntica posição manifestou a *Associação Nacional de Municípios Portugueses*, para quem a redação da proposta de lei é manifestamente desadequada ao nosso ordenamento jurídico.

O *Sindicato dos Jornalistas* entende que não deve o Estado Português reduzir a idade mínima para consentimento, dadas as evidências de que um menor de 13 anos é ainda "altamente influenciável e moldável na sua vontade, e por isso, imaturo nas suas decisões, devendo pois, quanto a este aspeto, ficar sujeito a proteção parental", sobretudo pela quantidade e diversidade de estímulos e capacidade de acesso a produtos/serviços no mercado digital.

Por outro lado, a *Associação Portuguesa de Marketing Direto, Relacional e Interativo* congratulou-se com a escolha dos 13 anos. Já a *Associação para a Promoção e Desenvolvimento da Sociedade da Informação*, apesar de concordar com o acesso ao mundo digital a partir dos 13 anos, por reconhecer as deficiências dos mecanismos de verificação da idade e o papel das crianças no desenvolvimento e mediação de tais serviços, recomenda a referência ao acompanhamento parental e à literacia de segurança e privacidade.

A *Associação dos Operadores de Comunicações Eletrónicas* (APRITEL) considera a idade mínima de consentimento como o "tema mais sensível e complexo de toda a Consulta, pois exige fazer uma difícil ponderação entre os riscos sobre a privacidade do menor e os riscos da sua exclusão social e digital", mas apoia o limite de 13 anos constante da proposta, bem como a promoção da "formação digital dos jovens". Numa posição com a qual nos identificamos, a APRITEL realça, por um lado, os riscos associados à "especial vulnerabilidade, credulidade e imaturidade" das crianças, mas por outro lado, o exercício dos direitos civis e de liberdade de expressão, a importância do acesso à informação na formação cívica dos mais jovens e o papel dos serviços da sociedade da informação na construção da personalidade do menor. Conclui a Associação que

atos ilícitos penais sobre a esfera física ou jurídica do menor e consentir em atos lícitos de utilização de dados pessoais".

a necessidade de obtenção de consentimento parental acima dos 13 anos, para além de efeito prático discutível, seria inadequada face à utilização destas ferramentas pelos menores nas várias facetas da sua vida e poderia inclusivamente causar "fossos digitais" entre os jovens que têm ou não o consentimento parental, bem como entre classes sócios-económicas.

3.3. Consentimento parental

Quando a criança tenha menos de 16 anos, determina o artigo 8.º n.º 2 do RGPD que "o responsável pelo tratamento envida todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível".

Na falta de estipulação quanto à forma de proceder a esta verificação, o Grupo de Trabalho do Artigo 29.º (GT29)[48] recomenda uma "abordagem proporcionada" e de observância do princípio da minimização de dados. Esta abordagem implica dois aspetos essenciais, realçados pelo GT29: por um lado, a limitação da quantidade de informação obtida, por outro lado a ponderação dos riscos inerentes ao tratamento e a tecnologia disponível. As medidas de verificação adotadas, dependentes de uma avaliação casuística do tratamento de dados em questão, devem evitar soluções "que envolvam, elas mesmas, uma recolha excessiva de dados pessoais". A título meramente exemplificativo, o GT29 propõe a verificação por correio eletrónico para tratamentos de baixo risco e outras medidas (como o pagamento de 0,01 EUR através de transferência bancária) para tratamentos de alto risco.[49]

[48] As orientações do Grupo de Trabalho do Artigo 29.º foram assumidas pelo atual Comité Europeu para a Proteção de Dados e estão disponíveis em https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

[49] Cf. orientações do GT29 (WP259), p. 30. O GT29 apresenta ainda o seguinte exemplo, elucidativo dos esforços adequados envidados pelo responsável pelo tratamento para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança: "[Exemplo 23] Uma plataforma de jogos em linha quer garantir que os clientes menores só conseguem subscrever os seus serviços com o consentimento dos progenitores ou tutores. O responsável pelo tratamento segue os passos seguintes:
Passo 1: pede ao utilizador que indique se tem menos ou mais de 16 anos (ou idade alternativa para consentimento digital).
Se o utilizador indicar que a sua idade é inferior à idade para consentimento digital:
Passo 2: o serviço informa a criança de que um dos progenitores ou tutores deve consentir ou autorizar o tratamento antes de o serviço ser prestado à criança. É pedido ao utilizador que revele o endereço eletrónico de um dos progenitores ou tutores.

Cumpre agora mencionar algumas questões conexas com a de definição da idade de consentimento digital.

a) A propósito do consentimento do *titular das responsabilidades parentais da criança*, interessa analisar a quem caberá dar ou autorizar tal consentimento. Como efeito da filiação, se estabelecida em relação a ambos, compete aos pais o exercício das responsabilidades parentais relativamente à pessoa e bens dos filhos.[50] Na constância do matrimónio (ou se os progenitores viverem em condições análogas às dos cônjuges[51]) esse exercício pertence a ambos os pais, de comum acordo, presumindo-se em regra[52] que se um dos pais praticar ato que integre o exercício das responsabilidades age de acordo com o outro.[53] A questão torna-se problemática quando o casamento "termina" (aqui se incluindo, para este efeito, as hipóteses de divórcio, separação judicial de pessoas e bens, declaração de nulidade e anulação do casamento[54], e ainda a separação de facto[55]), quando cessa a convivência entre os progenitores[56] ou quando estes não vivam em condições análogas às dos cônjuges[57]. A distinção faz-se, nos termos do artigo 1906.º do CC, entre as "questões de particular importância para a vida do filho" e os "atos da vida corrente do filho". Relativamente às questões de particular importância, as responsabilidades parentais são exercidas em comum por ambos os progenitores, salvo em casos de manifesta urgência ou determinação judicial que julgue contrário aos interesses do filho esse exercício em comum. Já quanto aos atos da vida corrente, o exercício das responsabilidades cabe ao progenitor que reside habitualmente com o filho ou ao progenitor com quem ele se encontra

Passo 3: o serviço contacta o progenitor ou tutor e obtém o seu consentimento através de mensagem de correio eletrónico para o tratamento e toma medidas razoáveis para confirmar que o adulto tem responsabilidade parental.
Passo 4: em caso de queixas, a plataforma toma medidas adicionais para verificar a idade do subscritor.
Se a plataforma observar os outros requisitos do consentimento, a plataforma pode cumprir os critérios adicionais do artigo 8.º do RGPD seguindo estes passos."

[50] Cf. artigos 1877.º e seguintes do Código Civil (CC).
[51] Por remissão do artigo 1911.º n.º 1 do CC.
[52] Esta presunção de consentimento não opera nos casos em que a lei expressamente exija o consentimento de ambos os progenitores ou se trate de ato de particular importância.
[53] Cf. artigos 1901.º e 1902.º do CC. Em caso de impedimento (artigo 1903.º) ou morte (artigo 1904.º) de um dos progenitores, o exercício das responsabilidades cabe, naturalmente, ao outro.
[54] Cf. artigo 1906.º do CC.
[55] Por remissão do artigo 1909.º do CC.
[56] Por remissão do artigo 1911.º n.º 2 do CC.
[57] Por remissão do artigo 1912.º n.º 1 do CC.

temporariamente, sendo que nesta última hipótese o progenitor não deve contrariar as orientações educativas mais relevantes definidas pelo progenitor com quem o filho reside habitualmente.[58] Cabe à doutrina e à jurisprudência preencher estes conceitos indeterminados.[59] Na exposição de motivos da alteração legislativa de 2008, que consagrou o atual regime, fica clara a intenção de que as questões de particular importância "se resumam a questões existenciais graves e raras, que pertençam ao núcleo essencial dos direitos que são reconhecidos às crianças".[60] No que se refere ao consentimento parental para o tratamento de dados do filho em relação aos serviços da sociedade da informação, a qualificação como "particular importância" ou "vida corrente" dependerá do tipo de dados pessoais e operação sobre eles efetuada, usualidade do tratamento, riscos a ele inerentes, consequências na vida futura da criança, idade do menor, etc., pelo que só em concreto se poderá aferir se a decisão de consentimento deve ser conjunta ou caber apenas ao progenitor com quem a criança se encontra. Por exemplo, o consentimento para a prática pontual de um jogo online poderá considerar-se um ato da vida corrente, mas já a decisão de ter ou não conta numa rede social ou um canal de YouTube exigirá a concertação dos progenitores.

b) Importa ainda saber quais as implicações, quanto ao consentimento prestado, do *titular dos dados atingir a idade mínima* de consentimento digital. O artigo 7.º n.º 3 do RGPD assegura o direito de retirada do consentimento a qualquer momento, possibilidade da qual o titular dos dados deve ser informado, e de modo a que seja "tão fácil de retirar [o consentimento] quanto de dar". Assim, ao atingir a idade mínima de consentimento digital, o titular dos dados pode confirmar, modificar ou retirar o consentimento anteriormente dado pelos titulares das responsabilidades parentais.

[58] Nos termos do n.º 4 do artigo 1906.º do CC, o exercício das responsabilidades parentais relativas ao ato da vida corrente pode ser delegado em terceiros. Já o mesmo não acontece relativamente às questões de particular importância.

[59] Cf. elenco exemplificativo do Guia Prático do Divórcio e das Responsabilidades Parentais (2.ª Edição), Centro de Estudos Judiciários, p. 74 e seguintes, disponível em http://www.cej.mj.pt/cej/recursos/ebooks/familia/guia_pratico_divorcio_responsabilidades_parentais.pdf.

[60] Cf. Exposição de Motivos do Projeto de Lei n.º 509/X, disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=33847.

c) O próprio legislador europeu ressalva, no Considerando 38, os "serviços *preventivos ou de aconselhamento* oferecidos diretamente a uma criança", no contexto dos quais não deve ser necessário o consentimento do titular das responsabilidades parentais. O GT29 exemplifica a prestação de serviços de proteção de crianças oferecidos em linha a uma criança através de um serviço de conversação em linha.[61]

d) Por último, a articulação da problemática do consentimento digital dos menores com as disposições nacionais de *direito contratual*. O artigo 8.º n.º 3 do RGPD especifica que o disposto em matéria de condições aplicáveis ao consentimento "não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança." Deste modo, não obstante o menor poder autonomamente dar o seu consentimento em matéria de serviços que lhe são diretamente oferecidos na sociedade da informação, a apreciação da validade de um eventual contrato celebrado online continua sujeita às regras gerais do Código Civil em matéria de incapacidade dos menores para o exercício dos direitos, designadamente a anulabilidade dos negócios jurídicos celebrados pelo menor (artigo 125.º do CC). Do mesmo modo, serão excecionalmente válidos os atos previstos no artigo 127.º daquele Código, incluindo os "negócios jurídicos próprios da vida corrente do menor que, estando ao alcance da sua capacidade natural, só impliquem despesas, ou disposições de bens, de pequena importância", como poderá ser o caso de alguns serviços de comunicações eletrónicas de tarifário limitado ou subscrição de determinados conteúdos digitais. Convém ressalvar aqui os *jogos e apostas online* (assim se entendendo os jogos de fortuna ou azar, apostas desportivas à cota e apostas hípicas, mútuas e à cota, quando praticados à distância, através de suportes eletrónicos, informáticos, telemáticos e interativos, ou por quaisquer outros meios), cujo regime jurídico nacional expressamente afasta do conceito de jogador os menores de idade.[62]

[61] Será disso exemplo, entre nós, a Linha SOS Criança, à qual a criança poderá recorrer sem prévia autorização parental.
[62] Cf. artigos 1.º e 4.º l) do DL n.º 66/2015, na sua versão atual.

4. Conclusões

A título de conclusão, apontamos quatro reflexões principais:

i) Em matéria de consentimento dos menores quanto ao acesso aos serviços da sociedade da informação e inerente tratamento dos seus dados pessoais, devem ser ponderadas soluções normativas e práticas que permitam equilibrar os perigos e potencialidades de tais serviços;

ii) Mais do que normas de cariz proibitivo e repressivo, importa apostar na prevenção e na capacitação (*empowerment*) dos jovens consumidores, através de políticas sólidas de educação para o consumo e literacia digital;

iii) A jusante da definição normativa, urge garantir a aplicação efetiva (*enforcement*) das medidas destinadas à proteção dos menores como titulares de direitos digitais;

iv) A tutela da infância, também no âmbito da exposição dos menores à publicidade e tratamento dos seus dados pessoais com finalidades de marketing, é uma responsabilidade partilhada entre famílias, sistema educativo, sociedade e Estado.

> *"It is hoped that businesses and governments alike will adopt measures to better protect and empower children as full rights-holders in a digital world"*[63]

REFERÊNCIAS

ALMEIDA, Susana - A Publicidade Infanto-Juvenil e o Assédio pela Internet. **Revista Luso-Brasileira de Direito do Consumo.** ISSN 2237-1168. Vol. IV, n.º #14, junho (2014), p.149-175.

AZEVEDO, Mário Gabriel de Castro Nunes - Tutela do consumidor menor de idade. O consumidor menor de idade e a publicidade. **Revista Portuguesa de Direito do Consumo.** ISSN 0873-9773. n.º 53, março (2008), p.56-88.

[63] Cf. UNICEF, Discussion paper series: Children's Rights and Business in a Digital World, "Privacy, Protection of Personal Information and Reputation", disponível em https://www.unicef.org/csr/ict_paper-series.html.

BRITTO, Igor Rodrigues - Crítica contra a publicidade infanto-juvenil brasileira. **Revista Portuguesa de Direito do Consumo**. ISSN 0873-9773. n.º 51, setembro (2007), p.64-116.

CANOTILHO, J. J. Gomes; MOREIRA, Vital - **Constituição da República Portuguesa - Anotada - Volume I - Artigos 1º a 107º.** 4ª edição revista. Coimbra: Coimbra Editora, 2007. ISBN 978-972-32-1462-8.

CARDOSO, António - Uma perspectiva parental sobre a influência das crianças na compra de vestuário. **Revista da Faculdade de Ciências Humanas e Sociais.** ISSN 1646-0502. n.º 2 (2005), p.162-190.

CARVALHO, Diógenes Faria de; OLIVEIRA, Thaynara de Souza - A Categoria Jurídica de 'Consumidor-Criança' e sua Hipervulnerabilidade no Mercado de Consumo Brasileiro. **Revista Luso-Brasileira de Direito do Consumo.** ISSN 2237-1168. Vol. V, n.º #17, março (2015), p.207-230.

GOMES, Carla Amado - O direito à privacidade do consumidor – A propósito da Lei 6/99, de 27 de Janeiro. **Revista do Ministério Público.** ISSN 0870-6107. Vol. 77, n.º Separata (1999), p.89-103.

GONÇALVES, Tamara Amoroso - A regulamentação da publicidade dirigida a crianças: um ponto de encontro entre o direito da criança e do adolescente e o direito do consumidor. **Revista Luso-Brasileira de Direito do Consumo.** ISSN 2237-1168. Vol. IV, n.º #14, junho (2014), p.121-147.

KARAGEORGIADIS, Ekaterine - Lanches Acompanhados de Brinquedos: Comunicação Mercadológica Abusiva Dirigida à Criança e Prática de Venda Casada. **Revista Luso-Brasileira de Direito do Consumo.** ISSN 2237-1168. Vol. IV, n.º #14, junho (2014), p.11-39.

MIRANDA, Jorge; MEDEIROS, Rui - **Constituição Portuguesa Anotada – Tomo I.** Coimbra: Coimbra Editora, 2005. ISBN 972-32-1308-7.